SIEMENS

SIMATIC NET

Industrial Ethernet OSM/ESM Network Management

User Manual

Preface, Contents

1 Introduction

2 Important OSM/ESM Functions

3 Command Interpreter (CLI)

4 Web-Based Management (WBM)

5 SNMP and RMON

6 Upgrading/Downloading Software

7 Notes on Troubleshooting

Appendix

A Internet Browser Settings

B Connecting a PC with Hyperterminal to the Serial Port of the OSM/ESM

C References

D Abbreviations/Acronyms

Glossar, Index

Release 11/2003

C79000-G8976-C137-08

Classification of Safety-Related Notices

This manual contains notices which you should observe to ensure your own personal safety, as well as to protect the product and connected equipment. These notices are highlighted in the manual by a warning triangle and are marked as follows according to the level of danger:

Danger

indicates that death or severe personal injury **will** result if proper precautions are not taken.

Warning

indicates that death or severe personal injury **can** result if proper precautions are not taken.

Caution

with warning triangle indicates that minor personal injury can result if proper precautions are not taken.

Caution

without warning triangle indicates that damage to property can result if proper precautions are not taken.

Notice

indicates that an undesirable result or status can occur if the relevant notice is ignored.

Note

highlights important information on the product, using the product, or part of the documentation that is of particular importance and that will be of benefit to the user.

Trademarks

SIMATIC®, SIMATIC HMI® and SIMATIC NET® are registered trademarks of SIEMENS AG.

Third parties using for their own purposes any other names in this document which refer to trademarks might infringe upon the rights of the trademark owners.

Safety Instructions Regarding your Product

Before you use the product described here, read the safety instructions below thoroughly.

Qualified Personnel

Only **qualified personnel** should be allowed to install and work on this equipment Qualified persons are defined as persons who are authorized to commission, to ground, and to tag circuits, equipment, and systems in accordance with established safety practices and standards.

Correct Usage of Hardware Products

Note the following:

Warning

This device and its components may only be used for the applications described in the catalog or the technical description, and only in connection with devices or components from other manufacturers which have been approved or recommended by Siemens.

This product can only function correctly and safely if it is transported, stored, set up, and installed correctly, and operated and maintained as recommended.

Before you use the supplied sample programs or programs you have written yourself, make certain that no injury to persons nor damage to equipment can result in your plant or process.

EU Directive: Do not start up until you have established that the machine on which you intend to run this component complies with the directive 89/392/EEC.

Correct Usage of Software Products

Note the following:

Warning

This software may only be used for the applications described in the catalog or the technical description, and only in connection with devices or software products from other manufacturers which have been approved or recommended by Siemens.

Before you use the supplied sample programs or programs you have written yourself, make certain that no injury to persons nor damage to equipment can result in your plant or process.

Prior to Startup

Before putting the product into operation, note the following:

Caution

Prior to startup you must observe the instructions in the relevant documentation. For ordering data of the documentation please refer to the catalogs or contact your local SIEMENS representative.

Copyright © Siemens AG 2001 All rights reserved

The reproduction, transmission or use of this document or its contents is not permitted without express written authority. Offenders will be liable for damages. All rights, including rights created by patent grant or registration of a utility model or design, are reserved.

Disclaimer of Liability

We have checked the contents of this manual for agreement with the hardware and software described. Since deviations cannot be precluded entirely, we cannot guarantee full agreement. However, the data in this manual are reviewed regularly and any necessary corrections included in subsequent editions. Suggestions for improvement are welcome.

Siemens AG
Automation and Drives
Postfach 4848, D-90327 Nürnberg

Subject to technical change.

Preface

OSM/ESM with Network Management

As of firmware version 2.0, all Industrial Ethernet OSMs (Optical Switch Modules) and Industrial Ethernet ESMs (Electrical Switch Modules) have integrated management functions.

These functions provide you with simple methods of modifying settings on OSMs/ESMs, monitoring OSMs/ESMs, and running network diagnostics. If you already have OSMs and ESMs, you can upgrade them with the network management functions by simply downloading new firmware via the serial port.

This user manual describes the functions of firmware version 2.3.5

Note

Upgrading OSMs version 1 (order number 6GK1105-0AA00) or ORMs is not possible.

The OSM/ESM allows three separate ways of using network management, all of which are possible at the same time:

- Web-Based Management (WBM); in other words, operation and diagnostics using an Internet browser.
- SNMP Management; in other words, parameter assignment and diagnostics from one or more management stations.
- A command interpreter (CLI - command-line interface) accessible both via the serial port of the OSM/ESM and using TELNET

With remote monitoring (RMON), the OSM/ESM provides you with a wide range of diagnostic functions for your network. You can, for example, record network load trends and visualize them on a network management console or you can configure the OSM/ESM to send traps (alarm messages) to notify you of faults and errors.

Note

To use SNMP management, RMON and traps, you require a network management station. This is not supplied with the OSM/ESM.

Using network management on the OSM/ESM, you can also configure a redundant coupling allowing several rings or networks to be interconnected redundantly.

Purpose of the Manual

This manual describes the network management functions of the Industrial Ethernet OSM/ESM. It explains network management with SNMP, Web-Based Management of OSM/ESM, and how to set parameters with the command interface.

Aims

With this manual, you should be in a position to use the network management functions of the OSM/ESM.

Scope of the Manual

This manual is valid for the OSM/ESM with firmware version 2.3 and higher.

Notes for the Reader

How you use the manual depends on what you want to do...

- You want to get to know the functions of the OSM/ESM. First, read the OSM/ESM manual supplied with the device on CD. This manual can also be downloaded from the SIMATIC Customer Support Web site under entry number 8677203 at http://www4.ad.siemens.de/view/cs/en/8677203.
- You want an overview of SNMP and Web-Based Management. Read the introduction in Chapter 1.
- You want to know how to use the integrated command interpreter (CLI). This is explained in Chapters 2 and 3.
- You want to control the OSM/ESM with an Internet browser or want to get diagnostic information from the OSM/ESM using a browser. You will find information on these topics in Chapters 2 and 4 of this manual. Trying out Web-Based Management is the simplest way of familiarizing yourself with the management functions of the OSM/ESM.
- You want to monitor the OSM/ESM from a network management station using SNMP or want to use the RMON functions of the OSM/ESM. Read Chapter 5 in this manual.

Finding Information

To help you to find the information you require more quickly, the manual includes not only the table of contents but also the following sections in the Appendix:

- Glossary
- References
- Index
- Abbreviations/Acronyms

References

References to other documentation are indicated by the reference number in slashes /.../. Based on these numbers, you can find the title of the documentation in the References at the end of the manual.

Target Group

This documentation is intended mainly for users and system administrators who want to use the network management functions of the OSM/ESM.

Audience

This manual is intended for persons with the qualifications required for installation, operation, and programming of the described product.

If you want to control the OSM/ESM using Web-Based Management, you must be familiar with the basic functions of an Internet browser and be capable of making changes to the browser settings. You will find information on the settings required in Web browsers in the appendix to this manual. It is also assumed that you are already familiar with the functions of the OSM/ESM as described in the OSM/ESM manual /1/.

If you want to access the OSM/ESM from a management station using SNMP or want to use remote monitoring (RMON), it is assumed that you are familiar with operating the management station (for example, HP Open View or SNMPc from Castle Rock) and that you know the basic mechanisms of SNMP and Ethernet switching.

Personnel Qualification Requirements

Only qualified personnel should be allowed to install and work on this equipment .

Qualified personnel as referred to in the operating instructions or in the warning notes are defined as persons who are familiar with the installation, assembly, startup and operation of this product and who possess the relevant qualifications for their work, e.g.:

- Training in or authorization for connecting up, grounding or labeling circuits and devices or systems in accordance with current standards in safety technology;
- Training in or authorization for the maintenance and use of suitable safety equipment in accordance with current standards in safety technology;
- First Aid qualification.

Possible Security Risks on Standard IT Interfaces

In various SIMATIC NET components such as OSM/ESM, a wide range of parameter assignment and diagnostic functions (for example Web Server, Network Management) are available over open protocols and interfaces. The possibility of unauthorized misuse of these open protocols and interfaces by third parties, for example to manipulate data, cannot be entirely excluded.

When using the functions listed above and these open interfaces and protocols (for example, SNMP, HTTP, Telnet), you should take suitable security measures to prevent unauthorized access to the components and the network particularly from within the WAN/Internet.

Caution

We expressly point out that automation networks must be isolated from the rest of the company network by suitable gateways (for example using tried and tested firewall systems).
We do not accept any liability whatsoever, whatever the legal justification, for damage resulting from non-adherence to this notice.

If you have questions on the use of firewall systems and IT security, please contact your local Siemens office or representative. You will find the address in the SIMATIC NET Catalog IK PI or on the Internet at http://www.siemens.de/simatic-net.

Further Support

If you have other questions on SIMATIC NET products, please contact your local Siemens office or representative. You will find the addresses in the SIMATIC NET Catalog IK PI or on the Internet at http://www.siemens.de/simatic-net.

Preface ..... **i**

1 Introduction **1-1**

1.1 Network Management with SNMP 1-2
1.1.1 Function 1-2
1.1.2 Communication 1-3
1.1.3 Management for Industrial Networks 1-4

1.2 Network Management for Industrial Networks 1-5
1.2.1 Signaling Concept 1-5
1.2.2 Network Management 1-5
1.2.3 Web-Based Management (WBM) 1-6

1.3 Command Interpreter (CLI) 1-8

1.4 Setting the IP Addresses 1-8

2 Important OSM/ESM Functions **2-1**

2.1 Autonegotiation 2-2

2.2 Autocrossover 2-3

2.3 Transmission Rate and Duplicity 2-3

2.4 Factory Defaults and Protected Settings 2-4

2.5 Filtering Database (FDB Table) 2-5
2.5.1 Entries in the FDB Table 2-5
2.5.2 Displaying and Deleting FDB Entries, Aging 2-6
2.5.3 Reaction to Spanning Tree Frames 2-6

2.6 Locked Ports 2-8

2.7 Mirroring 2-9

2.8 Traps 2-10

2.9 E-Mail Function 2-11

2.10 Event Log Table 2-12

2.11 Time of Day and Time-of-day Synchronization 2-13

2.12 Flow Control 2-14

2.13 BOOTP/DHCP 2-15

2.14 IP Configuration Using SIMATIC NET NCM PC, SIMATIC STEP 7 or the Primary Setup Tool 2-16

2.15 TELNET 2-17

2.16 Extended Redundant Configuration 2-18

2.17 Observer Function 2-21
2.17.1 Observer Error Messages 2-21

2.18 Automatic Download of the Configuration 2-23

2.2 Autocrossover 2-3

3 Command Interpreter (CLI) **3-1**

3.1 Overview 3-2

3.2 Password Protection 3-2
3.3 Installing the CLI 3-3
3.4 Login 3-4
3.5 CLI Commands 3-5

4 Web-Based Management (WBM) 4-1

4.1 General Introduction 4-2
4.1.1 Restricted Functionality of the OSM/ESM Variants 4-2
4.2 Requirements 4-3
4.3 Connecting 4-4
4.4 Access Using Web-Based Management 4-5
4.5 User Interface of Web-Based Management 4-7
4.6 Management Menus 4-9
4.7 System 4-10
4.7.1 System Version Numbers 4-11
4.7.2 System Restart 4-13
4.7.3 System Factory Defaults (restoring the defaults) 4-14
4.7.4 System Save & Load 4-15
4.7.5 Event Log Table 4-17
4.8 OSM/ESM Status 4-18
4.8.1 OSM/ESM Fault Mask 4-21
4.8.2 OSM/ESM Standby Mask 4-23
4.8.3 OSM/ESM Counters 4-25
4.9 Agent Features 4-27
4.9.1 Agent Event Configuration 4-29
4.9.2 Digital Input Configuration (only OSMs/ESMs with digital inputs) 4-30
4.9.3 Agent E-Mail Configuration 4-31
4.9.4 Agent Trap Configuration 4-33
4.9.5 Agent ARP Table 4-34
4.9.6 Agent SNMP Counters 4-35
4.10 Switch Features 4-36
4.10.1 Current FDB Table 4-38
4.10.2 Static FDB Table 4-40
4.10.3 FDB Unicast Configuration 4-41
4.10.4 FDB Multicast Configuration 4-43
4.11 Port Status 4-45
4.11.1 Port Configuration 4-47
4.12 Statistics Counters 4-49
4.12.1 Packet Size 4-50
4.12.2 Packet Type 4-51
4.12.3 Packet Error 4-52

5 SNMP and RMON 5-1

5.1 SNMP 5-2

5.2 RMON 5-3
6 Upgrading/Downloading Software 6-1
6.1 General Introduction 6-2
6.2 Downloading the Firmware via the Serial Port 6-3
6.3 Downloading Firmware from an TFTP Server 6-6
7 Notes on Troubleshooting 7-1
A Internet Browser Settings A-1
A.1 Microsoft Internet Explorer 6.0 . . . . . A-2
A.2 Netscape Communicator 6.2 . . . . . A-11
B Connecting a PC with Hyperterminal to the Serial Port of the OSM/ESM B-1
C References C-1
D Abbreviations/Acronyms D-1
Glossary Glossary-1
Index Index-1

1 Introduction

1.1 Network Management with SNMP

The Industrial Ethernet OSMs (Optical Switch Modules) and Industrial Ethernet ESMs (Electrical Switch Modules) have SNMP and Web Based Management. This chapter briefly explains the basics of network management with SNMP and Web-Based Management.

In the past, homogeneous office networks installed with components from one manufacturer could also be maintained and administered with the proprietary management systems provided by the manufacturer. Due to the constant increase in the size of networks and internetworking involving the widest variety of different network types (for example an intranet), these proprietary management systems often reach their limits.

The problem was solved in the eighties with the introduction of the Simple Network Management Protocol (SNMP) by the Internet Activities Board (IAB). This standard was readily accepted by the network industry and solves the essential tasks of a network management system.

1.1.1 Function

Client/Server Model

A network management system that uses SNMP works according to the client/server model. The management station or simply manager (client) can query status information from the components it is responsible for controlling. These components can be widely differing devices within the network system, such as network components, switches, hubs or DTEs such as workstations, PCs or network printers.

Agent

An **agent** (server) is installed on all of these devices. This agent that is normally implemented on the components as software functionality provides the **management system** with station-specific data or receives configuration data. Access to the components by the management station (both reading and writing) is cyclic and uses the **network management protocol** (SNMP).

The station data provided by the agent is stored in structured form in the **MIB** (**M**anagement **I**nformation **B**ase, see below).

The agent not only has the task of providing data when requested by the management station, but can also react event-driven by sending a message known as a trap to the management station.

Communication between the management station and agents involves only an insignificant increase in overheads on the network during operation.

1.1.2 Communication

Protocol

SNMP uses the connectionless protocol UDP (User Datagram Protocol).

Getting Information

To read the required status information, the manager sends a **Get** request to the agent of the device. The addressed component answers the request with a **Response** message.

Making Settings

To change the current configuration of a managed device, the manager sends a **Set** request.

Status changes can be notified to the manager event-driven and without polling by the agent sending a **Trap** message.

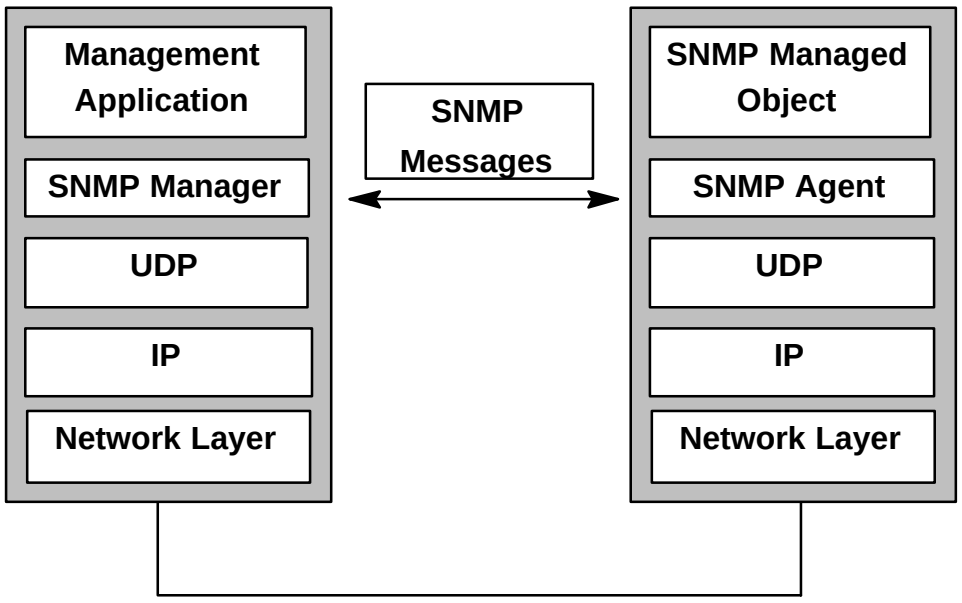


Figure 1-1 SNMP Communication

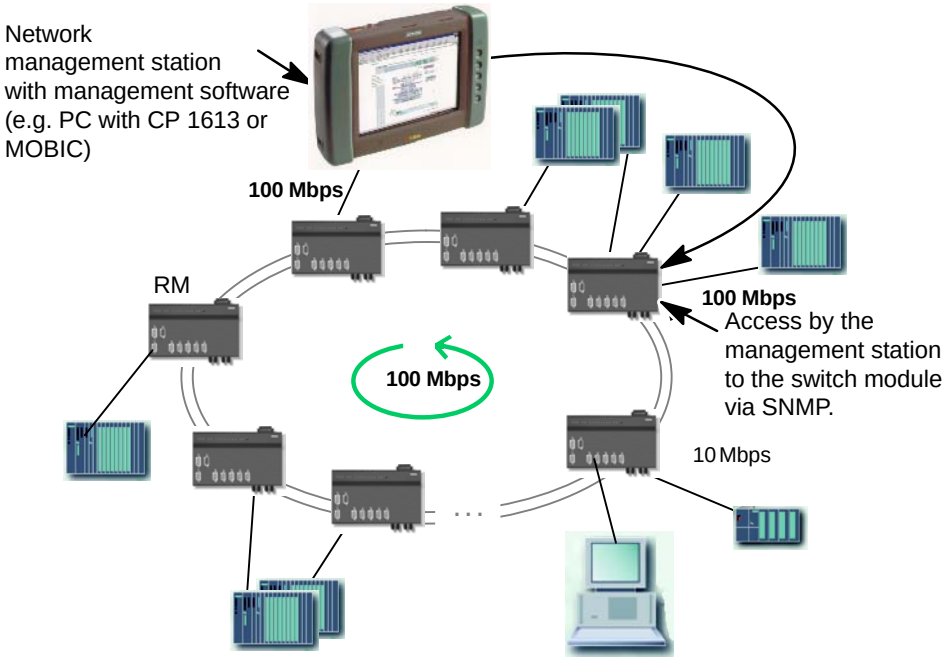


Figure 1-2 Communication Between a Management Station and Switch

1.1.3 Management for Industrial Networks

MIB

The MIB is a data structure made up of different variables (management objects) that can be polled or set by the management system. The variables used for polling are described in a language independent of the target system.

Thanks to the standardized MIBs and access mechanisms used by all manufacturers, it is possible to monitor and control a network with components from a wide range of vendors. Device views allow the management objects to be displayed graphically in the management system. If there is no device view available for the component, the objects are represented row-oriented using an MIB browser.

If additional data is required for network monitoring, this can be defined in private MIBs by the vendors. This allows values to be polled that are not included in the standard.

1.2 Network Management for Industrial Networks

The trend towards larger and larger structures in industrial networks has been apparent for some time. Vertical integration, in other words the growing together of industrial networks and office networks, allows transparent access to all data but also requires integrated diagnostic functions. To meet the new requirements of this situation, the SIMATIC NET signaling concept using a signaling contact has been extended to include network management.

1.2.1 Signaling Concept

All active Industrial Ethernet network components have a signaling contact. Using this digital contact, the network component provides a group signal with which various statuses can be reported. Using an input module, this signal can then be passed on to operator control and monitoring systems (for example WinCC) where it can be visualized. This allows problems in a network to be recognized early and eliminated. The signaling concept with a signaling contact is a reliable and adequate monitoring system for small and medium sized networks.

1.2.2 Network Management

For industrial networks extending over large company complexes and linked to office networks, the signaling concept outlined above is not always suitable for monitoring the network. Moreover, there are not always suitable I/O cards available that are capable of reading in these digital signals.

For such networks, SIMATIC NET provides network management functionality based on SNMP for network monitoring in the OSM/ESM product range.

This allows the new switch modules to be managed, monitored and tested with every network management tool available on the market, for example, HP Open View, SunNet Manager or SNMPc from Castle Rock.

1.2.3 Web-Based Management (WBM)

To allow users to introduce network management cost-effectively, Web-Based Management is available for network management and diagnostics with the SIMATIC NET switch modules.

With the aid of Web-Based Management, it is possible to address individual network nodes or DTEs using an Internet browser such as the Netscape Communicator or Internet Explorer. By using the browser technology, access to network nodes on different platforms such as WinNT or UNIX is possible. Since the user is generally familiar with a browser, network management can be learned quickly and easily.

To allow Web-Based Management, an applet is stored on the OSM/ESM modules from SIMATIC NET that is loaded with the browser. This applet accesses data from the MIB of the addressed module dynamically and represents it graphically in the browser.

Web-Based Management allows access to only one network node at a time. An overview of all the nodes in the network and their topological arrangement is possible only with an extensive SNMP-based network management tool.

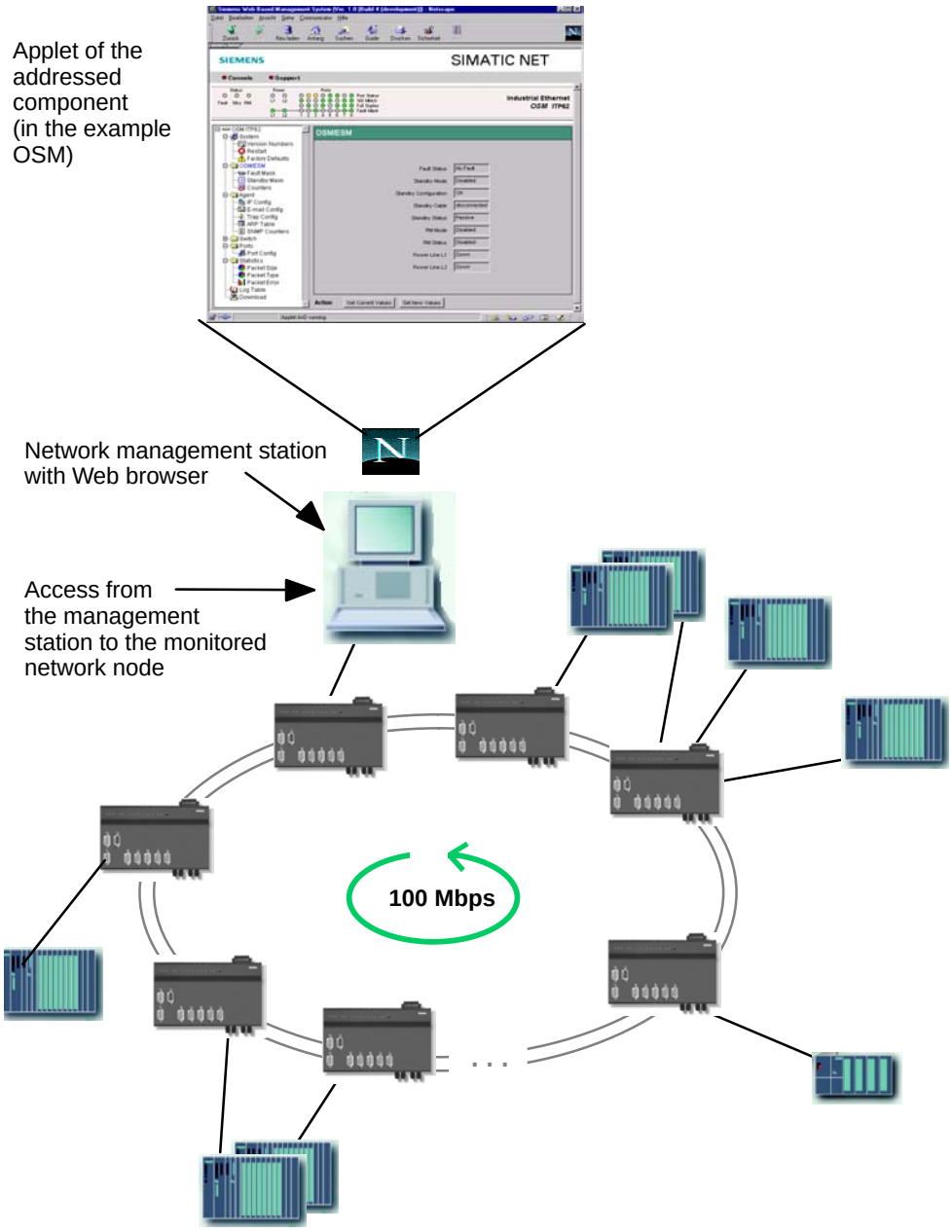


Figure 1-3 Industrial Network with Management System

1.3 Command Interpreter (CLI)

In addition to the Web-Based Management, you can also change or query all the important parameters of an OSM/ESM using a terminal with a V24 interface (for example a PC with the Windows Hyperterminal program). The terminal is connected to the serial port of the OSM/ESM. The functions of the OSM/ESM are manipulated using a simple command interpreter (CLI, Command-Line Interface). TELNET also provides the same functionality.

1.4 Setting the IP Addresses

You can set the IP configuration (IP address, subnet mask, gateway) using the following alternative methods:

- Manually using the Command Line Interface (Chapter 3)
- Manually using SIMATIC NET NCM PC, SIMATIC STEP 7 or the Primary Setup Tool (Section 2.14)
- Automatically using BOOTP/DHCP (Section 2.13)

When supplied, the OSM/ESM has no IP address and BOOTP/DHCP is activated.

To use Web Based Management, Telnet, SNMP, E-Mail, TFTP (saving/downloading configuration data, firmware update over Ethernet), the OSM/ESM must have an IP address.

2 Important OSM/ESM Functions

2.1 Autonegotiation

In the autonegotiation mode, an electrical OSM/ESM port sets itself automatically to the transmission rate (10/100 Mbps) of the connected partner device. If the partner device also supports autonegotiation, the devices further negotiate whether they will exchange data in the half-duplex or full-duplex mode and full-duplex flow control.

Note

If an OSM/ESM port that supports the autonegotiation mode is connected to a partner that does not support this mode, the port of the partner device must be set to the half-duplex mode.

2.2 Autocrossover

Electrical OSM/ESM ports with the autocrossover function are capable of crossing over the send and receive signals internally in the port. This means that straight-through or crossover TP cables can be used without causing problems.

To use the autocrossover function:

- At least one of the two ports must support the autocrossover function.
- The autonegotiation mode must be set on the port providing the autocrossover function.

OSM TP22, ESM TP40 and all OSMs/ESMs with order numbers ending in “10” (for example, 6GK1105-2AA10) provide autocrossover functionality.

Notice

Please note that even when using straight-through cables, an invalid loop can result in the Ethernet network, for example, by linking two ports on one OSM/ESM. Such a loop can lead to network overload and network failures.

2.3 Transmission Rate and Duplicity

The transmission rate and/or duplicity of the electrical ports can also be set by the user with network management functions. The values are shown in Table 2-1 below.

The transmission rate and duplicity of a port set by the user only comes into effect if autonegotiation is turned off for the port.

Table 2-1 Transmission Rate and Duplicity

Ports	Transmission Rate	Duplicity
Electrical ports	10 or 100 Mbps	Half duplex or full duplex
Optical ports	only 100 Mbps	Only full duplex

2.4 Factory Defaults and Protected Settings

Defaults

The OSM/ESM had default settings made in the factory (see 4.7.3Factory Defaults). The user can query and modify these defaults with WBM, the CLI or SNMP.

The screenshots of the WBM dialogs in Chapter 4 show the default settings. You will find further default settings in the private MIB file (see Section 4.7.3).

Restore Memory Defaults and Restart

Using WBM or the CLI, a command is available with which it is also possible to restore some of the factory defaults.
Apart from the protected settings, all the settings are restored to the factory setting.

Protected Settings

The protected settings of the OSM/ESM are not modified when you restore the factory defaults to avoid having to make settings again unnecessarily.

The protected settings are as follows:

IP address, subnet mask, default gateway, system name, system location, system contact.

Restore Factory Defaults

Using WBM or the CLI, a command is available with which it is also possible to restore the factory defaults. The factory defaults are also restored if you trigger a RESET with the button on the front panel of the OSM/ESM, see /1/.
The protected settings are also reset!

If you trigger the function using the CLI or WBM, the device does not start automatically. You will be prompted to start the device manually. Before you start manually, you have the opportunity of reconfiguring the device. To be able to communicate with the device later over the LAN, it is important to specify the IP address.

Notice

If the device operates as standby master or standby slave, and the user configuration of the linking signal lines does not match the default factory setting, make sure that you disconnect the signal line(s) before starting the “Factory Default” function.

2.5 Filtering Database (FDB Table)

The FDB (**F**iltering **D**ata**b**ase) table is used by the OSM/ESM to decide which port or ports a received packet is transferred to. The FDB table of the OSM/ESM can hold up to 7000 addresses.

2.5.1 Entries in the FDB Table

The FDB table contains two types of entries (addresses):

- Static MAC addresses: These can be entered and deleted by the user with WBM or SNMP.
- Learned MAC addresses: These are learned by the OSM/ESM automatically; in other words they are entered in the FDB table when the module receives corresponding packets. The OSM/ESM makes an entry in the FDB table indicating the port at which it learned the address; in other words, the port to which the node with the corresponding MAC address is connected. After making this entry, it then passes all received packets for this node to the relevant port. This mechanism reduces network load. Automatic learning is only possible when **lock disabled** is set for the relevant OSM/ESM port, see Section 2.6. This is the default setting.

Note

- The OSM TP22 and ESM TP40 do not support static entries in the FDB table.
- Static addresses are retained when the OSM/ESM is turned on and off or restarted; learned addresses are deleted.
- In the redundant manager (RM) mode, no static address entries are possible.
- No static unicast addresses can be entered for the ring ports.
- If a port is used for a redundant network link (master and standby link), there must be no static addresses entered for it.

2.5.2 Displaying and Deleting FDB Entries, Aging

The entries in the FDB table can be displayed by the WBM, see Section 4.10.1. Static addresses can also be entered or deleted in WBM.

If **aging** is activated (default), a **learned** entry (address) is automatically deleted in the FDB table when no packet with this source address is received within the **aging time**.

Aging prevents addresses that are no longer up to date from remaining in the FDB table permanently. “Aged entries” can, for example, mean that a node that has been connected to a different OSM/ESM port is no longer obtainable because the packets intended for it are still sent to the original port.

In WBM and in the CLI, aging can be enabled and disabled and the aging time can be modified. The default setting for the aging time is 40 seconds.

2.5.3 Reaction to Spanning Tree Frames

When an OSM/ESM is interfaced to a higher-level office network, users often require this interface to be implemented redundantly. The company network, however, uses third-party components that do not support fast OSM/ESM redundancy mechanisms (forming rings and standby links). At other points in the office network, a mesh topology is used and the resulting loops are eliminated by the spanning tree protocol (IEEE 802.1D).

As of firmware version 2.3.5, OSMs/ESMs are capable of evaluating spanning tree frames that report modified configurations in the office network. This allows an OSM/ESM ring to interface redundantly with an office network based on spanning tree.

During configuration changes (triggered by topology change events) made in a connected spanning tree office network, an OSM/ESM reduces its aging time. As a result, the MAC addresses of all stations (for example PCs) from which no further frames are received during this shortened time are removed from the address table. Stations that use new or modified network paths following a change in the configuration can therefore be reached again more quickly. On completion of the configuration changes, the OSM/ESM changes back to normal operation.

Note

The OSM/ESM passes on all spanning tree frames regardless of the function described above. The OSM/ESM itself does not send any spanning tree frames.

The times involved in configuration changes depend on the spanning tree configuration and the network topology. The actual time required to change the configuration must be determined based on tests.

During modification of a configuration, ”Configuration BPDUs” (configuration frames) with the ”TC” Flag (”topology change” bit) set are sent repeatedly in a connected spanning tree network . Based on these frames, an OSM/ESM recognizes the duration of the changes to the configuration.

2.6 Locked Ports

Locking

Locking is used to make sure that only packets from authorized stations are passed on by the OSM/ESM.

Lock Enabled

If the **lock enabled** function is activated for an OSM/ESM port, the OSM/ESM only passes on packets received at this port if the source address exists in the FDB table. All other packets are discarded. Learning new addresses is also disabled on this port; in other words, if a packet with a new source address is received, this address is not included in the FDB table of the OSM/ESM.

Addresses that have already been learned, are deleted automatically if aging is activated (see Section 2.5.2). A restart will force all learned addresses to be deleted immediately.

Lock Disabled

If **lock disabled** (default setting) is set, the OSM/ESM passes on packets with an unknown source address received at a port (in other words an address that does not exist in the FDB table of the OSM/ESM). New source addresses are automatically learned on this port; in other words, they are entered in the FDB table.

Programming Authorized Nodes

If you only want the packets from certain authorized nodes to be passed on by the OSM/ESM, follow the steps outlined below:

1. Enter the MAC addresses of these nodes and the number of the port to which they are connected in the FDB table of the OSM/ESM using WBM.
2. Set the port to **lock enabled**.
3. Run an OSM/ESM restart using WBM to delete the learned entries in the FDB table and to save the configuration. The static addresses in the FDB table are retained when you restart.

Note

- The ring ports cannot be configured with Lock enabled.
- If a port is used for a redundant network link (master and standby link), it must not be configured with Lock enabled.

2.7 Mirroring

Mirroring for Diagnostics

Mirroring allows you to mirror (copy) the bi-directional data traffic to an OSM/ESM port (mirrored port) to another OSM/ESM port (monitor port) and to record it with a protocol analyzer for diagnostic purposes.

Settings

You can set the mirrored and monitor port and activate the mirror function both with the command-line interface or using WBM. Ports 1 to 6 of the OSM/ESM can be used as the monitor port.
With the OSM TP22 and ESM TP40 variants, only ports 1 and 2 are permitted as the monitor ports.

Mirroring Active

If the mirroring function is activated and if the monitor port has a valid connection to the attached protocol analyzer, the port LED of the monitor port on the OSM/ESM flashes quickly (4 x short with pause).

Note

Please remember to turn off the mirroring function if you connect a normal DTE to the monitor port.

2.8 Traps

Trap Messages

If certain events occur, the OSM/ESM can generate (SNMP) trap messages and send them to up to 10 different nodes, for example management stations. By configuring the management station, the traps can be displayed on the user interface. An interpreted display is possible only when the corresponding MIB files can be evaluated by the management station. For example, to obtain a plain language display of special OSM/ESM functions, the private OSM/ESM MIB file must be loaded (see Section 4.7.3).

Issuing Traps

If the trap function is activated, traps are issued by the OSM/ESM automatically in the following situations:

Standard Traps (RFC 1157)

- After powering up or restarting.
- At link up, link down; in other words, when the valid connection to the DTE at a port is interrupted or reestablished.
- If an SNMP authentication error occurs; in other words, when a network management station or the Internet browser attempts to access the OSM/ESM using SNMP requests with the wrong access permission (community name).

RMON Traps (RFC 1757)

- When certain limit values are violated (high, low) that were configured earlier on the OSM/ESM by a network management station using RMON.

OSM/ESM-Specific Traps

- When the OSM/ESM ring is opened/closed by the redundancy manager (OSM/ESM in the RM mode), see /1/.
- When there is a switchover between the standby master and standby slave in a redundant coupling, see /1/.
- If the error state changes, see /1/.
- When one of the two power supplies of the OSM/ESM is turned on or off during operation.

Enabling/Disabling Traps

The issuing of traps can be enabled or disabled by WBM or the command-line interface.

2.9 E-Mail Function

The OSM/ESM has an E-mail function with which an E-mail can be sent automatically (for example to the network administrator) if an alarm occurs. If the E-mail function is activated, the OSM/ESM sends an E-mail in the same situations that lead to a trap being issued (see Section 2.8). The E-mail includes the identification of the sending OSM/ESM and a description of the cause of the alarm in plain language. For networks with only a few nodes, this allows simple centralized network monitoring to be implemented on the basis of an E-mail system. When an E-mail fault message arrives, the WBM can be started by the browser based on the identification of the sender so that further diagnostic information can be obtained.

To use the E-mail function, the following requirements must be met:

- The E-mail function is activated on the OSM/ESM and the E-mail address of the recipient is configured.
- The E-mail function is activated for the particular event (event configuration, activated for all events as default).
- There is an SMTP server in your network that can be reached by the OSM/ESM.
- The IP address of the SMTP server is entered on the OSM/ESM.

The E-mail function can be activated by WBM or the command-line interface.

Note

Depending on the properties and configuration of the SMTP server, it may be necessary to adapt the “From” box for the E-mails. Please check with the administrator of the SMTP server. You can specify the “From” box using WBM, CLI or by direct SNMP access.

Unless modified, the OSM/ESM uses the following address:

<device_type>@<IP_address>

For example, OSM_ITP62@192.168.0.10

2.10 Event Log Table

Events are entered chronologically in the event log table (log book) of the OSM/ESM.

The events include:

- all events reported, including those via E-mail and trap,
- additional error messages if an E-mail server (SMTP) is not accessible or rejects the E-mail of an OSM/ESM.

The event log table can be read out using the command line interface (see section 3.5) over the Web Based Management (see Section 4.7.5) or using direct SNMP access. It can hold a maximum of 200 entries. When the number of entries reaches 201, the oldest entry is deleted (ring buffer).

2.11 Time of Day and Time-of-day Synchronization

The OSM/ESM has two times:

1. System Up Time:
   The time since the OSM/ESM was last restarted. The system up time is added to every E-mail and every entry in the event log table. After 497 days, the system up time starts again at 0. This oberflow results from the range of values of the standard MIB object (OID 1.3.6.1.2.1.1.3).
2. Date and Time of Day:
   The date and time of day can be set on the OSM/ESM either manually using a CLI command or automatically using SIMATIC time-of-day frames. Once the date and time of day have been set after restarting the device, the date an time-of-day information is added to E-mails and every event in the event log table. The date and time of day are NOT buffered if the device is turned off.

The OSM/ESM evaluates the cyclic multicast frames of a SIMATIC time transmitter and sets the date and time of day accordingly. This allows an absolute time to be assigned to reported events.

2.12 Flow Control

Flow control is a mechanism that reduces the risk of data loss in the network resulting from overload.
The OSM/ESM supports two flow control mechanisms:

- **Half Duplex Flow Control (Back Pressure)** for ports operating in the half duplex mode. With this type of flow control, the OSM/ESM reduces the packet rate received at a port if there is overload in the network by generating additional collisions.
- **Full Duplex Flow Control** complying with the IEEE 802.3x standard for ports operating in the full duplex mode. If there is overload, the OSM/ESM generates pause packets that stop or re-enable the sending of new packets by the connected partner device. This is only possible when the DTE supports full duplex flow control.

Half and full duplex flow control can be activated separately for each port of the OSM/ESM. If the OSM/ESM port is operating in the autonegotiation mode, the devices automatically negotiate whether or not the full duplex flow control is activated. It is also possible to deactivate flow control for all ports of the OSM/ESM at the same time.

Note

As default, full duplex flow control is deactivated. If you activate this, remember that this can delay time-of-day synchronization frames.

2.13 BOOTP/DHCP

If there is a BOOTP or DHCP server in your network, the OSM/ESM can automatically obtain the following from the server:

- the IP address,
- the subnet mask,
- the IP address of the default gateway,
- the IP address of the TFTP server,
- the configuration file (Section 2.17) / or the firmware file name

If the BOOTP/DHCP function is activated on the OSM/ESM (default), BOOTP and DHCP are always started after starting up the device.

BOOTP and DHCP can only be activated/deactivated together. When started, the OSM/ESM sends both BOOTP and DHCP frames. If a BOOTP and a DHCP server reply in the network, the DHCP server will be given priority by the OSM/ESM.

Note

The BOOTP/DHCP process delays the startup of the device by approximately 40 seconds if the BOOTP/DHCP server is not obtainable. For this reason, BOOTP/DHCP is deactivated as soon as an IP address is set using WBM, CLI, direct SNMP access or the Primary Setup Tool.

Note

DHCP provides a mechanism that allows a client to lease an IP address for a limited lease time. When the lease time expires, the OSM/ESM can no longer be contacted using its previous IP address. If you use DHCP, please check the (default) settings of the DHCP server regarding the lease time.

2.14 IP Configuration Using SIMATIC NET NCM PC, SIMATIC STEP 7 or the Primary Setup Tool

Just as several other SIMATIC NET products, the OSM/ESM also supports IP configuration (IP address, subnet mask, gateway) using SIMATIC NET NCM PC, SIMATIC STEP 7 or the Primary Setup Tool.
For more detailed information, refer to the documentation of the relevant product.

Note

- SIMATIC NET NCM PC and SIMATIC STEP 7 support IP configuration as of version 5.2. To configure an IP address, the SOFTNET for Industrial Ethernet option is also required.
- Assigning the IP address 0.0.0.0 to an OSM/ESM using SIMATIC NET NCM PC, SIMATIC STEP 7 or the Primary Setup Tool has the effect that BOOTP/DHCP is activated and BOOTP/DHCP is started immediately (without a restart of the device).
- Changes to the IP configuration using SIMATIC NET NCM PC, SIMATIC STEP 7 or the Primary Setup Tool become valid immediately without a restart on the OSM/ESM.
  In contrast, changes to the IP configuration or to BOOTP/DHCP using the Command Line Interface, Web Based Management or SNMP only take effect after a restart of the device.
- The Primary Setup Tool is available from Siemens Automation and Drives Service & Support on the Internet under entry ID 14929629. You will find this entry at:
  http://www4.ad.siemens.de/view/cs/de/14929629

2.15 TELNET

With TELNET, you can operate the CLI of the OSM/ESM via the LAN/Internet. You can start a TELNET link to the OSM/ESM, for example, by clicking on the console icon in the login window of the OSM/ESM WBM, see Chapter 4.

Note

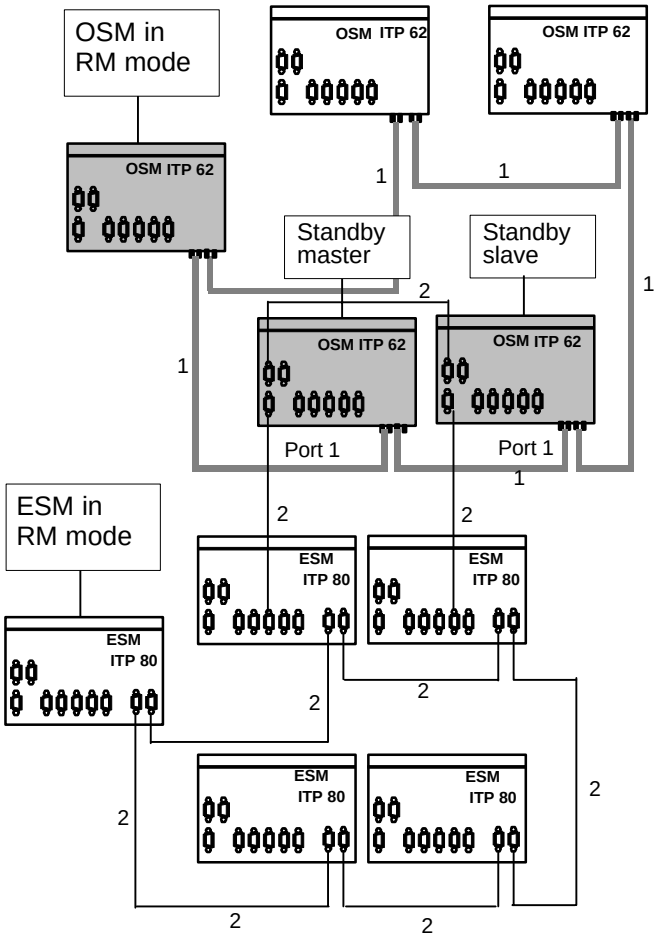
A maximum of 3 CLI links (serial + LAN) are possible at the same time.

2.16 Extended Redundant Configuration

Redundant Coupling

With OSMs/ESMs (except for the OSM TP22 and ESM TP40), you can implement redundant links, see /1/. A redundant coupling is created using two OSMs/ESMs, one of which is set to the standby slave with the DIP switch (”Stby on”) while the other operates as the standby master. The standby-sync ports of both OSMs/ESMs are interconnected using an ITP XP standard cable 9/9, see Figure 2-1.

In the factory default setting, port 1 is monitored by the standby master. In problem-free operation, data are transferred to the neighboring ring (network) via this port while there is no data exchange via port 1 of the standby slave. If the standby master fails or if there is a break on the link to port 1 of the standby master, the standby slave takes over data exchange.



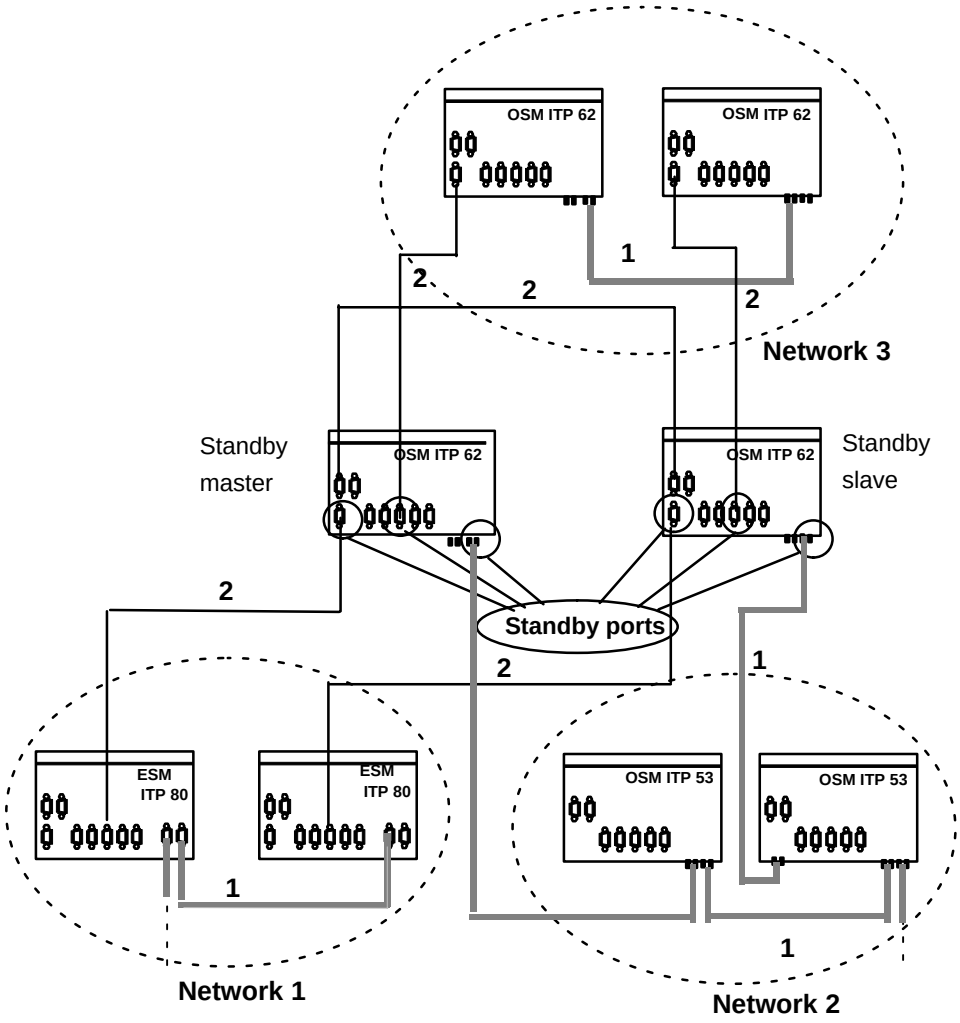
1 Fiber-optic cable (FO)
2 ITP XP standard cable 9/9

Figure 2-1 Redundant Coupling of Network Segments

Extended Redundant Configuration with Network Management

The extended redundant configuration of the OSM/ESM (with the exception of the OSM TP22 and ESM TP40) allows up to 8 rings or networks to be coupled redundantly with two OSMs/ESMs (see also /1/)

With network management (for example in WBM), each port of the standby master and standby slave can be configured as a standby port, see Figure 2-2. The other ports can be used as “normal” OSM/ESM ports.



1 Fiber-optic cable (FO)
2 ITP XP standard cable 9/9

Figure 2-2 Extended Redundant Configuration

In problem-free operation, only the standby ports of the standby master are active and handle data exchange. If the standby master or the link of one of the standby ports of the master fails, **all** standby ports of the master are disabled and the standby ports of the slave activated so that a functioning configuration is re-established.

Note

Please remember that the same ports on the standby master and standby slave must be configured as the standby ports. If an optical port of the OSM ITP62 (order number 6GK1105-2AA00)is used in an extended redundant coupling, it must have at least hardware version 2.

2.17 Observer Function

The observer function provides further opportunities for error diagnostics and error protection for redundant rings. It allows malfunctions of the redundancy manager or bad configuration of a redundant ring to be monitored. The Observer is also capable of opening the connected ring when the errors are detected (portection mode). The function is optional and as default deactivated.

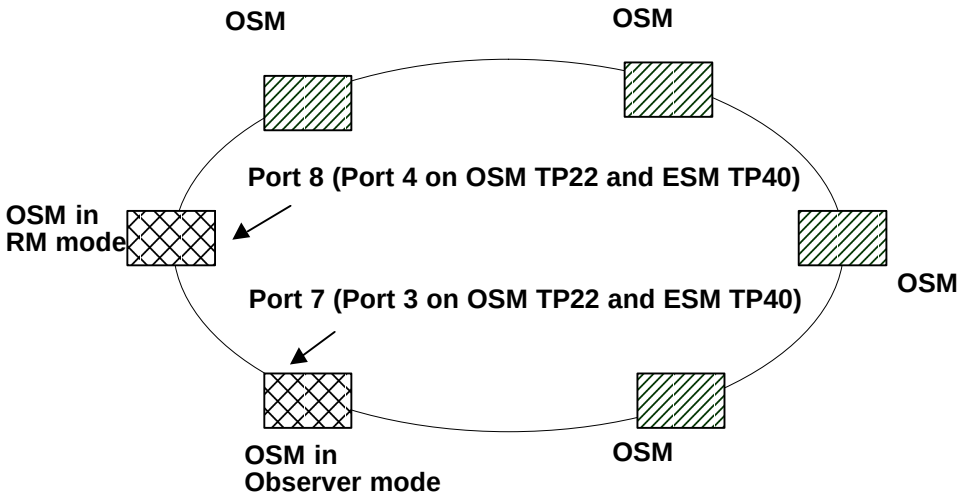


Figure 2-3 Redundant Ring Structure with Monitoring of the RM by the Observer

When creating a ring with the Observer, remember the following:

- The second ring port of the redundancy manager (port 8 on 8-port OSMs/ESMs, port 4 on 4-port OSMs/ESMs) must be connected with the first ring port of the Observer (port 7 on 8-port OSMs/ESMs, port 3 on 4-port OSMs/ESMs) (see Figure 2-3).
- The OSM/ESM acting as the observer must be switched to the observer mode using the Command Line Interface (CLI), the command syntax for the observer is explained in Chapter 3.
- The firmware version of both the observer and redundancy manager must be V2.2 or higher.

2.17.1 Observer Error Messages

Observer error messages are signaled using the method (path) selected for alarm events (Fault State Change - see Agent Event Configuration). These methods are E-mail, trap and/or event log table entry. The message text is: “Observer detected error”.

The status (see Table 2-2) is entered in the event log table and can also be displayed in the CLI OSM menu with the ”Info” command. The display may be delayed by several seconds.

Table 2-2

Status	Meaning	Possible Cause	Remedy
disabled ([1])	Observer function is disabled.		
starting ([1])	The Observer is waiting for test frames from the RM.	The Observer was started but no RM was found.	Check the cable and device functions as well as the correct wiring between the Observer and RM.
monitoring ([1])	The Observer monitors the RM function. This is the normal state.		
rm error : hardware fault([2]) rm cfg/hardware error rm error : test frames missing rm error : rm status mismatch ([2])	Error in the functioning of the RM	Bad wiring , device and/or wiring defective	Check the wiring between the Observer and RM according the instructions. Check whether cable and device function correctly. Problem indicators are the traffic and RM LEDs and the statistics counters of the ring ports.
cfg error : more than one observer	There is more than one Observer in the ring.	More than one Observer in the ring.	Check the device configuration. Only one device may be configured as the Observer in the ring!
cfg error : more than one rm	There is more than one RM in the ring.	More than one RM in the ring.	Check the device configuration. Only one device may be configured as the RM in the ring!
cfg error : rm sw-version	The firmware on the RM is incompatible.	Incompatible software versions of Observer and RM devices	Check the software version of the RM.
cfg error : rm on wrong port	The RM is connected to the wrong port of the Observer.	Wiring error	Connect the Observer to the RM as described in the instructions.
rm timeout	The Observer is no longer receiving test frames.	Device and/or wiring fault/error	Check whether cable and device function correctly. Problem indicators are the traffic LEDs and the statistics counters of the ring ports.

([1]): do not appear in the event log table.

([2]): in the protection mode, in addition to the event log entry, port 7 (port 3 on the OSM TP22 ESM TP40) is set to passive

2.18 Automatic Download of the Configuration

If the file name and folder of a configuration file is specified on the BOOTP server or DHCP server, the BOOTP/DHCP client of the OSM/ESM can trigger an automatic download of the configuration data over TFTP.

Requirements

The BOOTP and TFTP servers must be configured and started on the same station under one IP address. BOOTP must be activated on the OSM.

The following additional settings are necessary:

- on the BOOTP server or DHCP server:

  The file name of the configuration file and path to the folder

- On the OSM:

  The entered name of the configuration file corresponds to the factory setting “Not Defined Yet”.

When an OSM/ESM is started with the factory settings, a BOOTP query is started. The OSM/ESM then receives the following information from the BOOTP server:

- IP address, subnet mask and default gateway of the OSM/ESM
- IP address of the TFTP server (identical to the IP address of the BOOTP server)
- File name of a firmware or configuration file.

The OSM/ESM then loads the first bytes (identification data) of the file ”file name” from the TFTP server and checks whether this is a suitable configuration file based on this identification data. If the file is suitable, this OSM/ESM configuration is accepted by the OSM/ESM and the file name is saved as the “Configuration File Name”. If the file is not suitable, the OSM/ESM assumes that the file name supplied via BOOTP/DHCP is a firmware file and enters it as the firmware file name.

When the OSM/ESM restarts, the configuration file is not automatically loaded because the name of the configuration file is stored on the OSM/ESM and does not correspond to the factory setting “Not Defined Yet”.

Note

Please note that the IP configuration received from the BOOTP server or DHCP server is retained and the IP configuration from the configuration file is not adopted. The IP configuration contained in the configuration file is only adopted when the file is loaded manually.

3 Command Interpreter (CLI)

3.1 Overview

The CLI is required for the following:

- To **set the IP address** and the subnet mask of the OSM/ESM. This information is necessary so that the OSM/ESM is obtainable with SNMP, Web-Based Management or TELNET.
- To **assign new passwords** for the OSM/ESM.
- To read or modify OSM/ESM parameters as an alternative to SNMP or Web-Based Management.

The CLI can be accessed via the serial port of the OSM/ESM or using TELNET. (The OSM/ESM must already have an IP address/subnet mask. After a new IP address has been assigned, TELNET must be restarted.)

Note

To make sure that your last configuration changes are saved, use the “Restart” command in the CLI or WBM before you turn off the power to the device. All configuration changes are entered in the flash memory after approximately one minute or following a restart.

3.2 Password Protection

Access using the CLI is **password-protected**. You can log in as administrator or as user (with different passwords). An administrator can read and modify OSM/ESM parameters, a user can only read OSM/ESM settings (see Service menu in Section 3.5)

3.3 Installing the CLI

The CLI is accessible via the serial port of the OSM/ESM or via TELNET.

Serial Port

Connect a PC (or if preferred a VT100 operator terminal) to the serial port of the OSM/ESM. Use the Hyperterminal program available under Windows on the PC. (Please refer to the instructions in Appendix B of this manual).

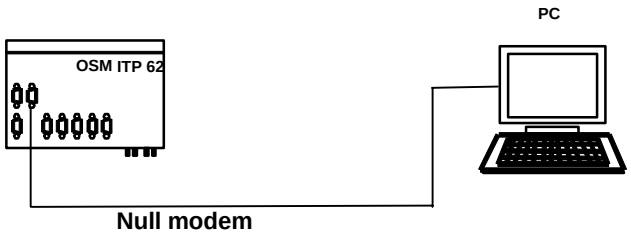


Figure 3-1 CLI Via the Serial Port

CLI via TELNET

The CLI functions are also available using TELNET, see Figure 3-2. The OSM/ESM must already have a valid IP address and a subnet mask. If the operator PC is in a different subnet on the OSM/ESM, the default gateway must also be configured on the OSM/ESM before access is possible using TELNET.

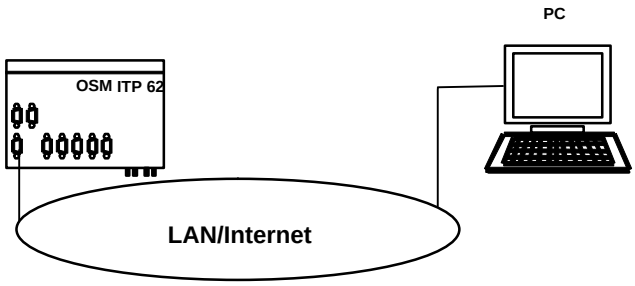


Figure 3-2 CLI via TELNET

A TELNET link to the OSM/ESM can, for example, be started in the login window of Web-Based Management by clicking on the console icon, see Chapter 4.

3.4 Login

Once the connection has been established via the serial port or using TELNET, the following prompt appears:

Login:

Type in **admin** (for administrator) or **user** (for user) according to your access permission and then press **[Return]**.

Password:

Enter your administrator or user password and press **[Return]**.

Note

If no new passwords were assigned (factory default), the valid password is **admin** for administrator and **user** for user.

If the password is lost, the OSM/ESM can be reset to the default values by pressing the button on the front panel, see Section 2.4. The passwords admin or user are then valid again.

Please note that after logging in via the serial port, commands can be entered until you log out with the exit command. Disconnecting the cable does not close the session.

The CLI then displays the start menu and the prompt

```
CLI>
```

You can now activate the commands of the CLI.

3.5 CLI Commands

This section explains the commands of the CLI, their functions and syntax.

Commands

The commands that are available depend on the access level; in other words, whether you logged in as user or as administrator. Table 3-2 contains an overview of the commands available for the administrator and user. The command-line interface provides functions comparable with those available in Web-Based Management. You should therefore also refer to the detailed explanations of the parameters available in Web-Based Management in Chapter 4.

Symbols

Table 3-1 explains the symbols used with the CLI commands.

Table 3-1 Symbols of the CLI Commands

Symbol	Meaning
<>	Mandatory entry
|	Used to separate possible alternative input values in a command. The factory default is shown on the extreme left. Only one of the possible values can be selected. Example: **aging <E|D>**: You must either enter **aging E** (aging enabled) or **aging D** (aging disabled), **E** is the default.
[ ]	Optional parameters. These options are used, for example, to be able to address several port numbers at the same time. The individual optional extensions are separated by commas; you can address groups using dashes. Example: If you enter the numbers 2,5- 8 in the [ports] field of a command, this command applies to ports 2 and 5 to 8.
()	Description of the commands.

Fast Input

To enter a command quickly, write the first letter or letters and then press the **[Tab]** key. If the required command is not shown, press the **[Tab]** key again.

Example

The following example illustrates how to use CLI commands.

Example:
The command **status <E | D> [ports]** is used to enable or disable OSM/ESM ports. The user enters the following: **status** followed by a blank and then the mandatory setting either **E** (= enable) or **D** (= disable) and then the optional port numbers as described in Table 3-1. If you do not enter a port number, the command applies to all ports.

- To enable the ports 2, 3, 4 to 6:
  Enter **status E 2,3,4-6** and confirm with **[Return]**.
- To disable ports 1 and 4 to 6:
  Enter **status D 1,4-6** and confirm with **[Return]**.

Note

The example refers to the 8-port variant of the OSM/ESM.

CLI Menus and Description

The following tables contain the commands, CLI menus and a brief description. If there are several alternatives for a command parameter, the default is always the value to the extreme left.

Start Menu

You can display all the other menus from the start menu. This is displayed immediately after you login and includes the following commands:

Table 3-2 Commands in the Start Menu

Command	Description	Comment
/	Returns you to the start menu (available in every menu)	
?	Displays the current menu again (available in every menu)	
restart	Restarts the OSM/ESM (available in every menu).	Administrator only.
exit	Closes the CLI/TELNET session. (available in every menu.)	
info	Displays status information about the OSM/ESM.	For explanations of the displayed parameters, see below or refer to the glossary.
SYSTEM	Opens the SYSTEM menu.	The SYSTEM menu is used to set the system parameters and to download the OSM/ESM firmware over a TFTP server.
OSM	Opens the OSM/ESM menu.	You make the OSM/ESM-specific settings (for example fault mask) in the OSM menu.
AGENT	Opens the AGENT menu.	You can enter the settings for network management (for example IP address) in the agent menu.
SWITCH	Opens the SWITCH menu.	You can make global settings for the OSM/ESM in the switch menu.
PORT	Opens the PORT menu.	The port menu is used to set the parameters of the OSM/ESM ports.
SERVICE	Opens the SERVICE menu.	In the SERVICE menu, you can change the password for CLI/TELNET.

System Menu

In the System menu, you can make settings required for downloading new OSM/ESM firmware from a TFTP server and for other system functions.

Table 3-3 Settings in the System Menu

Command	Description	Comment
info	Displays the current system settings.	For explanations of the displayed parameters, see below or refer to the Glossary.
defaults	Restores the defaults of the OSM/ESM (complete reset).	Administrator only The protected settings are also reset to their default values.
memreset	Restores the defaults of the OSM/ESM. The device is automatically restarted.	Administrator only This command restores the factory settings of the OSM/ESM. With the exception of the ”protected settings” (see Section 2.4), the settings made by the user are reset to the default values.
setsysc<string>	Sets the syscontact MIB variable. (To insert a blank in a string, use the tilde (~) instead of a blank.)	Administrator only
setsysl <string>	Sets the syslocation MIB variable. (To insert a blank in a string, use the tilde (~) instead of a blank.)	Administrator only
setsysn <string>	Sets the sysname MIB variable. (To insert a blank in a string, use the tilde (~) instead of a blank.)	Administrator only
time [date] [time]	With this command, you can display or set the date and time of day of the OSM/ESM. Example: time MM/DD/YYYY hh:mm In the display of the date and time of day, you can also see when it was set. An (m) after the date/time of day means that it was set manually. A (t) means that it was set by a time-of-day frame but that it is not synchronized. A (s) means that it was set via time-of-day frame and that it is synchronized with time transmitter.	Only the administrator can change the date and time of day.
events <show | clear>	Show | Clear content of the event log table.	Only the administrator can deleted the event log table. The event log table contains all the events that (when enabled) cause traps or E-mails. Other fault/error events such as communication errors are also logged with the SMTP server. The content of the event log table is retained even when the OSM/ESM is turned off.

Table 3-3 Settings in the System Menu

Command	Description	Comment
addlog <text>	This command makes an entry in the log of the OSM/ESM. To insert a blank in a string, use the tilde (~) instead of a blank.	Administrator only
server <IP address>	Sets the IP address of the TFTP server from which the new firmware for the OSM/ESM will be downloaded.	Administrator only
fwname < filename>	Enters the name of the file on the TFTP server containing the new OSM/ESM firmware (max. 32 characters) possibly including further path information (depending on the configuration of the TFTP server). To enter a name with blanks, use the tilde (~) instead of a blank.	Administrator only
fwload	Starts the firmware download from the TFTP server.	Administrator only
cfgname <filename>	Enters the name (max. 32 characters) under which the OSM/ESM configuration is loaded or stored as a file on the TFTP server. Depending on the configuration of the TFTP server, this may also include further path names. To enter a name with blanks, use the tilde (~) instead of a blank.	Administrator only
cfgsave	Stores the OSM/ESM configuration as a file on the TFTP server.	Administrator only
cfgload	Loads the OSM/ESM configuration as a file from the TFTP server.	Administrator only
logname <file name>	Enters the name (max. 32 characters) under which the OSM/ESM log is stored as a file on the TFTP server. Depending on the configuration of the TFTP server, this may also include further path names. To enter a name with blanks, use the tilde (~) instead of a blank.	Administrator only
logsave	Saves the OSM/ESM log as a file on the TFTP server.	Administrator only

OSM/ESM Menu

This menu includes special OSM/ESM settings, for example setting the fault mask.

Table 3-4 Settings in the OSM Menu

Command	Description	Comment
info	Displays the current values of the OSM/ESM setting.	For explanations of the parameters, see below or refer to the Glossary.
link <E | D> [ports]	Enable | Disable link monitoring.	Administrator only Link monitoring is part of the fault mask of the OSM/ESM, see /1/. The signaling contact and the fault LED of the OSM/ESM are activated when a port whose link monitoring is activated has no valid link.
power <E | D> [lines]	Enable | Disable monitoring of the power supply lines L1 and L2. Example: power E 1,2 enables monitoring for both power supply lines.	Administrator only Monitoring of the power supply lines L1 and L2 is part of the fault mask of the OSM/ESM, see /1/. The signaling contact and fault LED are activated when there is no voltage on a monitored power supply line or when the voltage is too low (less than 14 V).
standby <E | D> [ports]	Enable | Disable standby ports see Section 2.16. This command specifies which ports are standby ports.	Administrator only Not for OSM TP22 and ESM TP40
counters	Displays the results of the OSM/ESM counters. Meaning of the counters: **Changes to RM active state**: Indicates how often the OSM/ESM acting as RM closed the ring. **Max. delay of RM test packets**: Indicates (in ms) the maximum delay of the test packets sent by the RM. (The delay should not exceed 50 ms.) **Changes to Standby active state**: Indicates how often a standby slave took over the data exchange in a redundant coupling (see 2.16 **Signaled faults**: Indicates how often the signaling contact of the OSM/ESM was activated, see /1/	
resetc	Resets the OSM/ESM counters.	Administrator only

Table 3-4 Settings in the OSM Menu, continued

Command	Description	Comment
observer <E | D | R | P>	Start the Observer without the protection mode (enable), deactivate the Observer (disable), restart the Observer (restart), and start the Observer with the protection mode activated (protect). The operating status of the Observer can be read out using the Info command.	Administrator only

Agent Menu

The agent menu includes settings required to access the OSM/ESM using an Internet browser, SNMP management or TELNET.

Table 3-5 Settings in the Agent Menu

Command	Description	Comment
Info	Displays the current agent settings.	For explanations of the displayed parameters, see below or refer to the Glossary.
ip <IP address>	Enters the Internet protocol address of the OSM/ESM. The IP address is entered as usual in four fields each with a maximum of 3 decimal digits separated by periods, for example: 142.11.7.53	Administrator only The IP address must be entered if you want to access the OSM/ESM using an Internet browser, TELNET or SNMP. The IP address can also be assigned automatically by BOOTP/DHCP.
subnet <IP address>	Subnet mask. The subnet mask is entered as usual in 4 fields each with a maximum of 3 decimal digits separated by periods, for example: 255.255.0.0.	Administrator only The subnet mask must be entered if you want to access the OSM/ESM using an Internet browser, TELNET or SNMP.
gateway <IP address>	Sets the default gateway IP address, address format see above.	Administrator only The gateway IP address must be entered if you want to access the OSM/ESM via a gateway.
smtp <IP address>	Sets the IP address of the SMTP server, address format see above.	Administrator only
email <address>	Enters an E-mail address to which messages, for example alarms can be sent (up to 50 characters). The entry is in the standard format user@host.domain	Administrator only
mail <D | E>	Disable | Enable the E-mail function, see Section 2.9	Administrator only
from <address>	Sets the “from” field (up to 50 characters) of the E-mail function.	Administrator only Default OSM@ <IP-address> or ESM@<IP-address>, see Section 2.9.
bootp <D | E>	Disable | Enable BOOTP/DHCP, see Section 2.13.	Administrator only
rmon <D | E>	Disable | Enable RMON, see Section 5.	Administrator only Not for OSM TP22 and ESM TP40
telnet <E | D>	Enable | Disable TELNET,see Section 2.15.	Administrator only

Table 3-5 Settings in the Agent Menu

Command	Description	Comment
snmp <E | D>	Enable | Disable SNMP.	Administrator only SNMP must be enabled if you want to access the OSM/ESM with the Internet browser or using SNMP.
traps <E | D>	Enable | Disable traps, see Section 2.8.	Administrator only
showtrap	Shows the current trap configuration.	
settrap <entry> <IP> <E| D>	Sets a trap recipient as an entry in the trap configuration. entry: Trap entry 1 - 10 IP: IP address of the trap recipient Enable | Disable this trap recipient.	Administrator only
setrmon	This command is only used internally to store and load the configuration.	Administrator only Not for OSM TP22 and ESM TP40
getcomm <string>	Sets a read-only community string (up to 32 characters). The default is *public*.	Administrator only
setcomm <string>	Sets a read-write community string (up to 32 characters). The default is *private*.	Administrator only
ping [count] [size] <IP>	Sends a ping to the specified IP address. Example: ping -c 10 -s 128 192.168.1.1 Ten (count) pings with a frame length (size) of 128 bytes are sent to IP address 192.168.1.1.	
showec	Shows the current event configuration.	
setec <event> <E | D><E | D><E | D>	Sets an entry in the event configuration. Enable | Disable this entry.	Administrator only
showdis	Shows the state of the digital inputs of the device.	Only OSM/ESM with digital inputs
showdic	Shows the configuration of the digital inputs of the device.	Only OSM/ESM with digital inputs
setdname <input> <name>	With this function, you can assign a symbolic name (string) with a length of up to 64 characters to each digital input. (To insert a blank in a string, use the tilde (~) instead of a blank.) Example: setdname 5 doorcontact Assigns the symbolic name doorcontact to digital input 5 of the OSM BC08.	Administrator only Only OSM/ESM with digital inputs

Table 3-5 Settings in the Agent Menu

Command	Description	Comment
setdic <input> <E | D> <E | D> <E | D>	With this function, you can set the event configuration of the digital inputs. Enable/disable mail, trap, log Example: setdic 5 E E E If digital input 5 is set, an E-mail is sent, a trap is sent, and an entry is made in the log.	Administrator only Only OSM/ESM with digital inputs

Switch Menu

In the switch menu, you can make global settings for the OSM/ESM.

Table 3-6 Settings in the Switch Menu

Command	Description	Comment
info	Displays the currently active settings in the switch menu.	For explanations of the displayed parameters, see below or refer to the Glossary.
aging <E | D>	Enable | Disable aging.	Administrator only When aging is activated, a land address is automatically deleted in the FDB table of the OSM/ESM if no packet is received from the station with the relevant MAC address within the aging time.
agetime <seconds>	Setting for the aging time in seconds. The default is 40 seconds.	Administrator only
fdbpoll <seconds>	Sets the interval at which the copy of the filtering database kept internally on the OSM/ESM is updated.	Administrator only For service purposes only
mirror <D | E>	Enable | Disable mirroring.	Administrator only Mirroring allows the data exchange at one OSM/ESM port (mirrored port) to be mirrored to another port (monitor port) where it can be recorded with a protocol analyzer, see Section 2.7
m_ports <src> <dest>	Selects ports for ”mirroring”, see Section 2.7. ***src*** – (mirrored) port, i.e. the port whose data exchange will be recorded. (The default is 2) ***dest*** – (monitor) port, i.e. the port to which the protocol analyzer is connected. (The default is 1)	Administrator only
baud <9600 | 19200 | 38400 | 115200>	Sets the transmission rate of the serial port. The default is 115200.	Administrator only
flow <D | E>	Enable | Disable the flow control for all OSM/ESM ports, see Section 2.12.	Administrator only
find < MAC address >	Finds a MAC address in the FDB table of the OSM/ESM. Also specifies the ports to which a received packet with this (destination) address is sent.	The address must be entered in hexadecimal with blocks of two hexadecimal digits separated by hyphens, for example: 09:-00:-06:-01:FF:EF
lt	Displays the content of the FDB table of the OSM/ESM, see Section 2.5.	The addresses are displayed in hexadecimal. The ports to which the address is assigned are also displayed.
macuni <MAC> <port>	Sets a static entry of a unicast address in the address table.	Administrator only

Table 3-6 Settings in the Switch Menu

Command	Description	Comment
macmulti <MAC> <port1,port2,..>	Sets a static entry of a multicast address in the address table.	Administrator only
macerase <MAC address>	Deletes a static entry of an address in the address table.	Administrator only

Port Menu

In this menu, you can make port-specific settings for the individual OSM/ESM ports.

Table 3-7 Settings in the Port Menu

Command	Description	Comment
info [port]	Displays the current settings of the OSM/ESM ports. The actual status of the ports.	For explanations of the displayed parameters, see below or refer to the Glossary.
cfg [port]	Displays the configured settings of the OSM/ESM ports. The desired status of the ports.	
stat <S|T| E | clear> [port]	Shows the counter readings - of the frame length (**S**) - of the frames (**T**) - of the errors (**E**) of the selected port. The counters are reset with **clear**. Examples: show S 1,3-5 Shows the frame length of ports 1 and 3 through 5.	
name <port > <string>	With this function, you can assign a symbolic name (string) with a length of up to 64 characters to each OSM/ESM port. (To insert a blank in a string, use the tilde (~) instead of a blank.) Example: **name 5 Management~Port** Assigns the symbolic name Management Port to port 5 of the OSM/ESM.	Administrator only
status <E | D> [port]	Activate | Deactivate OSM/ESM ports. Deactivated OSM/ESM ports are disabled for data exchange.	Administrator only
fd_flow <E | D> [port]	Enable | Disable full duplex flow control.	Administrator only This flow control is effective when the selected ports operate in the full duplex mode and when flow control is activated in the Switch menu.
autoneg <E | D> [port]	Enable | Disable autonegotiation.	Administrator only Only the 10BASE T/ 100BASE TX ports can be switched to the autonegotiation mode.

Table 3-7 Settings in the Port Menu

Command	Description	Comment
lock <E | D> [port]	Enable | Disable the Lock port property, see Section 2.6.	Administrator only
hd_flow <E | D> [port]	Enable | Disable half duplex flow control.	Administrator only This flow control is effective when the selected ports operate in the half duplex mode and when flow control is activated in the Switch menu.
speed <? |10H |10F…> [port]	Displays | Sets transmission rate/ duplicity of the ports ***?*** displays the possible settings for the transmission rate and duplicity of the ports. 10H - - set 10 Mbps, half duplex. 10F - - set 10 Mbps, full duplex. 100H - - set 100 Mbps, half duplex. 100F - - set 100 Mbps, full duplex.	Administrator only (The transmission rate and duplicity of a port set by the user only takes effect if autonegotiation is disabled for this port. When autonegotiation is disabled, the transmission rate and duplicity of an OSM/ESM port must match the transmission rate and duplicity of the connected partner device.

Service Menu

Table 3-8 Settings in the Service Menu

Command	Description	Comment
info	Shows the basic settings of the OSM/ESM such as the MAC address, IP address, hardware and firmware versions.	
passwd [admin | user]	Allows the entry of a new password for the administrator or user.	Administrator only

4 Web-Based Management (WBM)

4.1 General Introduction

The OSM/ESM includes integrated Web-Based Management; in other words, it can be operated using an Internet browser. The modules are operated using a Java applet stored on the OSM/ESM that is loaded by the browser. To access the OSM/ESM, the IP address must be entered in the address field of the browser. If there is a DNS server in your network that can interpret the address of the OSM/ESM, you can also access the module using the logical name.

4.1.1 Restricted Functionality of the OSM/ESM Variants

OSM TP22 **ESM TP40**	- These OSM/ESM variants support only four ports. - Only four digital inputs are supported. - RMON is not supported. - Extended redundant coupling is not supported. - No FDB configuration
OSM TP62, **OSM TP62-LD,** **OSM ITP62,** **OSM ITP53,** **ESM TP80,** **and** **ESM ITP80** **with order numbers ending in “00” e.g. 6GK1105-2AA00**	- No digital inputs.

4.2 Requirements

To access an OSM/ESM using WBM, the following requirements must be met:

Internet Browser

You require a PC with an Internet browser. As the Internet browser, we recommend a **Netscape Communicator, Version 4.7** or a **Microsoft Internet Explorer, Version 5.0 or higher**.

Before your Internet browser will work with the OSM/ESM, you must make the correct settings in the browser. For more information, refer to Appendix A of this manual.

Address Settings

If you operate your OSM/ESM in the same subnet as your PC/Internet browser, you must first make the following settings via the CLI (serial port of the OSM/ESM):

- The **IP address** of the OSM/ESM. (The IP address can be set with the CLI command **ip <IP address>** , see also Section 3.5). As an option, the IP address can also be assigned automatically using a BOOTP server, see also Section 2.13.
- The **subnet address** of the OSM/ESM (CLI command subnet **< IP address>**, see also Section 3.5).

If your PC/Internet browser is in a different subnet from the OSM/ESM (subnets connected by a router), you must also set:

- The **default gateway** of the OSM/ESM (CLI command gateway **< IP address>**).

  As an option, these parameters can also be loaded from a BOOTP/DHCP server.

4.3 Connecting

Connect the Internet browser station and the OSM/ESM with the following configuration.

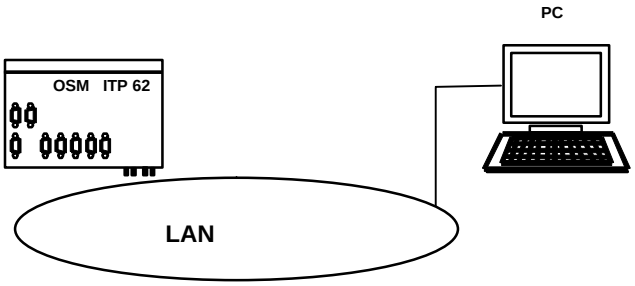


Figure 4-1 Internet Browser Connection

4.4 Access Using Web-Based Management

You can access the OSM/ESM using WBM as follows:

1. Open the Internet browser.
2. Enter the IP address or the URL of the OSM/ESM in the address box of the Internet Browser as follows:

   http://<IP address of OSM/ESM> e.g. http://142.11.7.8

   and confirm with **[Return]**.
3. When the “Login” window appears (Figure 4-2), select **admin** or **user** in the **Login ID** box (to select the access level). If you log in as administrator (**admin**), you have both write and read access; in other words you can change settings on the OSM/ESM. As user, you only have read access; in other words you can read out settings, counter values etc. but cannot modify them.

Figure 4-2 “Login” Window

In the login window, you can also establish a TELNET link to the OSM/ESM by clicking the console icon. If you click the support or SIEMENS icon, you automatically open the A&D home page.

4. Now enter the **password** and confirm by clicking the OK button.

Note

If no new passwords have been assigned, the valid password is the default **admin** (to use WBM as an administrator, for example with write/read permissions) and **user** (to use WBM as a user with read permissions only).

The admin and user passwords can only be modified via the CLI, see 3.5.

If you lose the password, you can reset the OSM/ESM to the original defaults with the button on the front panel, see Section 2.4. The admin or user passwords are then valid again.

As a reaction to the login, a web applet is loaded from the OSM/ESM. The following WBM startup window is displayed (see Figure 4-3).

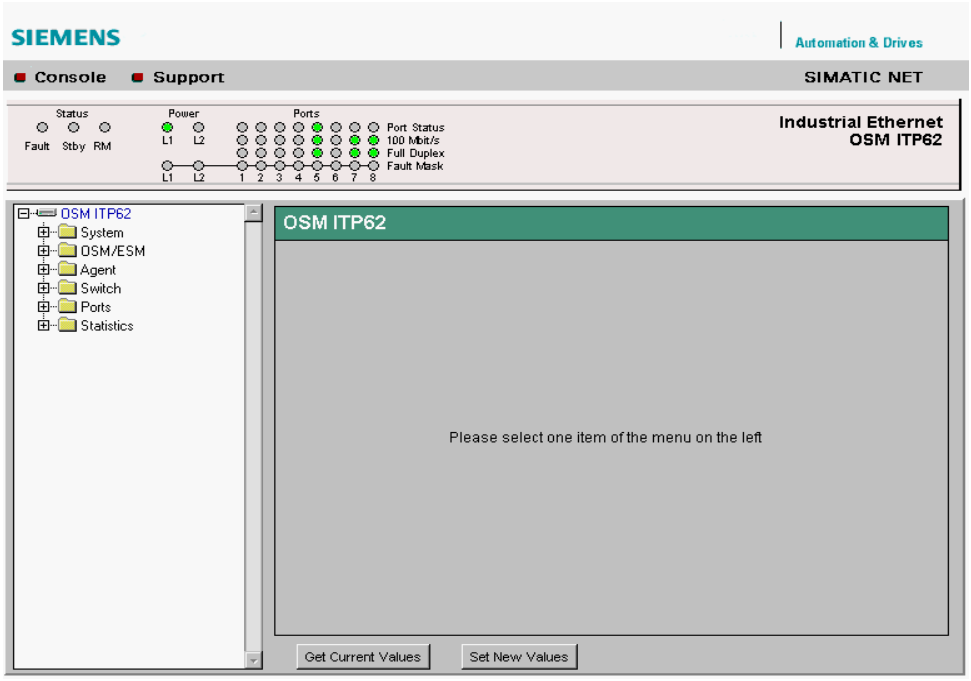


Figure 4-3 WBM Startup Window

4.5 User Interface of Web-Based Management

The dialogs of the OSM/ESM WBM are made up of a device status field, a menu tree, and a data window.

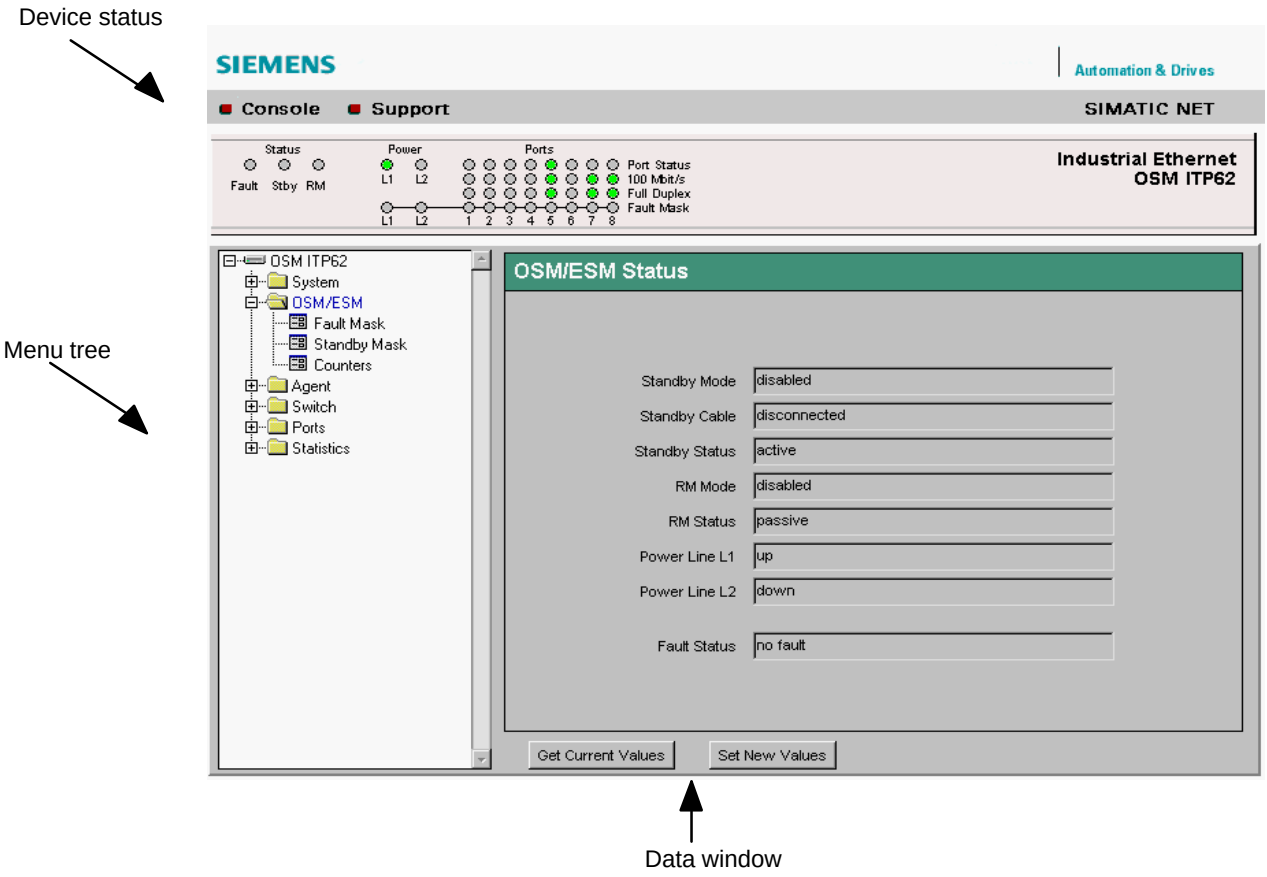


Figure 4-4 SIMATIC NET Network Management User Interface of the OSM/ESM

Device Status Field

The displays in the device status field correspond to the LEDs of the OSM/ESM, see /1/. The swapping over of the meaning of the port LEDs and the power LEDs (with the display button) is not implemented. Instead of this, the transmission rate, duplicity and the fault mask are represented by a separate row of LED symbols.

The signaling is identical to the LED signaling of the OSM/ESM, see /1/. The device status field is displayed and updated in every menu so that you have an overview of the current status of the OSM/ESM at all times.

The device status field also shows the OSM/ESM type (for example, OSM ITP53) and the system name (or the IP address if “sysName Not Set”) of the OSM/ESM.

On the OSM BC08, OSM TP22, and ESM TP40, the states of the digital inputs are also indicated on the right bedside the port LEDs.

Menu Tree

By navigating through the menu tree, you can open the individual windows of the OSM/ESM WBM in much the same way as when working in the Windows Explorer by clicking the relevant icons.

Data Window

The data window displays the current values and allows you to enter new settings. Settings that cannot be modified are displayed in gray.

4.6 Management Menus

The WBM of the OSM/ESM has the following menu structure:

System	Version Numbers Restart Factory Defaults Save & Load Event Log Table
OSM/ESM	Fault Mask Standby Mask Counters
Agent	Event Configuration Digital Input Configuration (only OSMs/ESMs with digital inputs) E-Mail Configuration Trap Configuration ARP Table SNMP Counters
Switch	Current FDB Table Static FDB Table FDB Unicast Configuration FDB Multicast Configuration
Ports	Port Configuration
Statistics	Packet Size Packet Type Packet Error

The menu commands and their windows are described in the following sections.

4.7 System

Clicking the **System** menu opens the window shown in Figure 4-5.

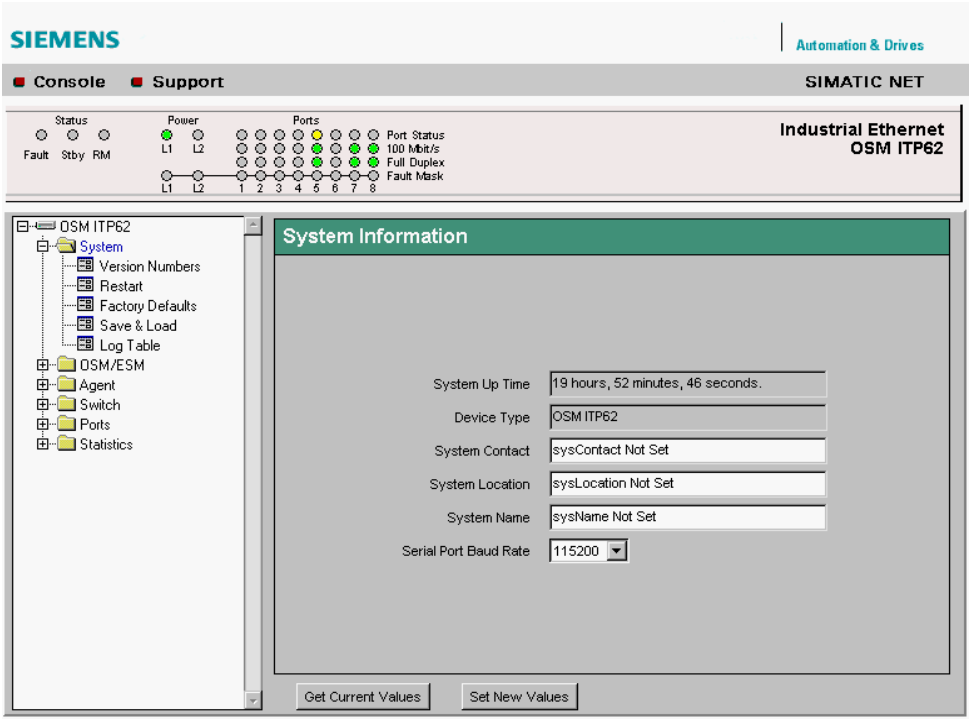


Figure 4-5 System Information Window

System Up Time

This shows the operating time of the OSM/ESM since the last restart.

System Description

The System Description box displays the OSM/ESM type.

System Contact

In this box, you can enter a contact person/address (for example the maintenance engineer) for this device (maximum 64 characters).

System Location

In this box, you can enter information about the location of the OSM/ESM (maximum 64 characters).

System Name

The domain name of the OSM/ESM can be entered in this field (maximum 64 characters).

Serial Port Baud Rate

This is the baud rate at which the serial port of the OSM/ESM operates. The default baud rate is 115.2 Kbauds.

Set New Values

To save the entries made in this window, click the **Set New Values** button. If you click the **Get Current Values** button, you obtain the values currently stored on the OSM/ESM.

4.7.1 System Version Numbers

Clicking the **Version Numbers** menu opens the window shown in Figure 4-6. This menu displays the hardware/software versions of the OSM/ESM, the order number and the MAC address of the OSM/ESM.

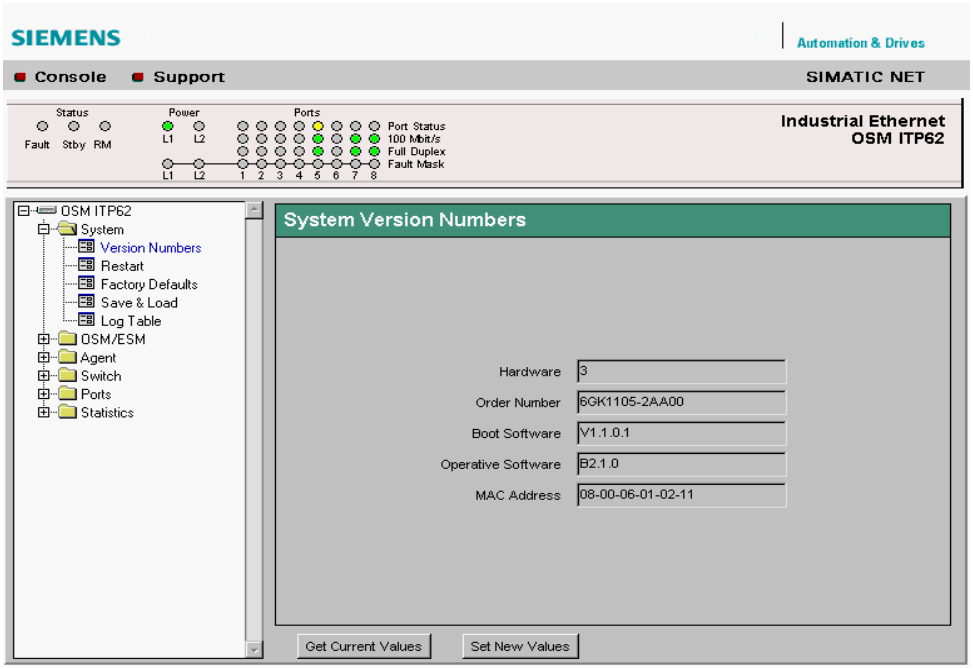


Figure 4-6 System Version Numbers Window

Hardware

Hardware version of the OSM/ESM.

Order Number

Order number of the OSM/ESM.

Boot software

Version of the boot software of the OSM/ESM. The boot software of the OSM/ESM is used to download new firmware (operative software) to the OSM/ESM and is stored permanently on the OSM/ESM.

Operative software

Version of the firmware currently loaded on the OSM/ESM.

MAC Address

MAC address of the OSM/ESM in hexadecimal format.

4.7.2 System Restart

With the **System Restart** window (Figure 4-7), you can restart the OSM/ESM.

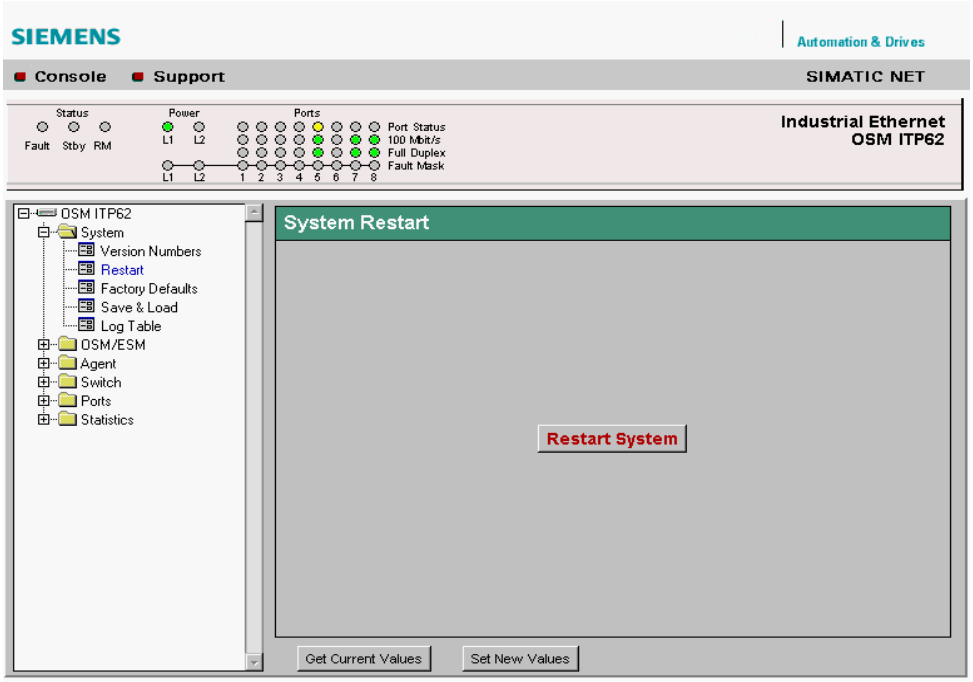


Figure 4-7 System Restart Window

To restart the OSM/ESM, click the **Restart System** button. This opens a dialog box in which you are prompted to confirm the “Restart” command. When you restart, the OSM/ESM is reinitialized, the internal firmware is reloaded and a self test is performed on the OSM/ESM hardware. The learned entries in the FDB table of the OSM/ESM are also cleared, see Section 2.5.1. Booting the OSM/ESM following a restart takes approximately 20 seconds. You can leave the browser window open while the OSM/ESM starts up.

4.7.3 System Factory Defaults (restoring the defaults)

Figure 4-8 shows the **Factory Defaults** window.

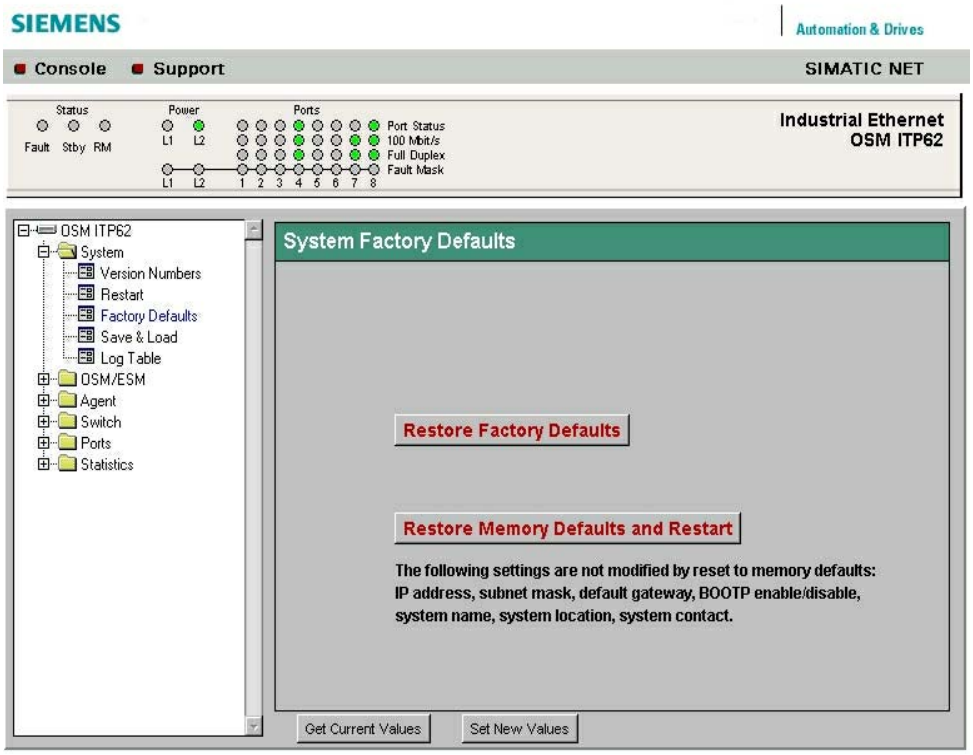


Figure 4-8 System Factory Defaults Window

In this window, you can restore the factory default settings for the OSM/ESM.

Restore Factory Defaults

The settings made in the factory are restored. Even the protected settings (see Section 2.4) are reset. There is no restart so that new data can be entered with the WBM. The changes only take effect when a manual restart is triggered, see also Section 4.7.2.

Restore Memory Defaults and Restart

The settings made in the factory are restored. This does not include the protected defaults (see Section 2.4) that are not affected by this command. A restart is triggered automatically.

4.7.4 System Save & Load

In the Save & Load window, you make the entries required to download the firmware for the OSM/ESM from a TFTP server. The settings for downloading and saving the OSM/ESM configuration and saving the event log table as a file over TFTP can also be made here.

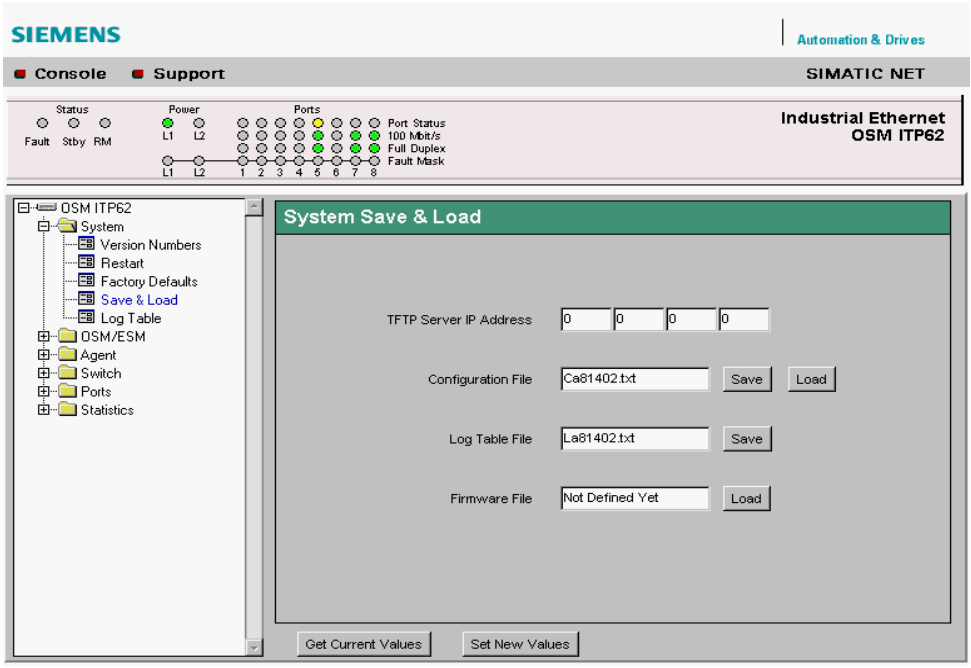


Figure 4-9 System Save & Load Window

TFTP Server IP Address

IP address of the TFTP server from which the new OSM/ESM firmware or a configuration file will be downloaded.

Configuration File

Name of the configuration file (maximum 32 characters) that is loaded from the TFTP server with the **Load** button or saved on the TFTP server with the **Save** button.

Log Table File

Name of the log table file (maximum 32 characters) that is saved on the TFTP server with the **Save** button.

If you do not enter a name for the configuration file and log table file, a file name based on the IP address is used.

Firmware File

Name of the file on the TFTP server containing the new OSM/ESM firmware (maximum 32 characters), if necessary with additional path information (depending on the configuration of the TFTP server). Clicking the **Load** button starts the download.

Note

If a configuration file of an RM was saved and then loaded on a normal OSM/ESM, the OSM/ESM fault mask for the ring ports is set. Manual reconfiguration may be necessary.

4.7.5 Event Log Table

The event log table (Figure 4-10) contains all the events that (if enabled) cause traps or E-mails. Other fault/error events such as communication errors are also logged with the SMTP server. The content of the event log table is therefore retained even when the OSM/ESM is turned off.

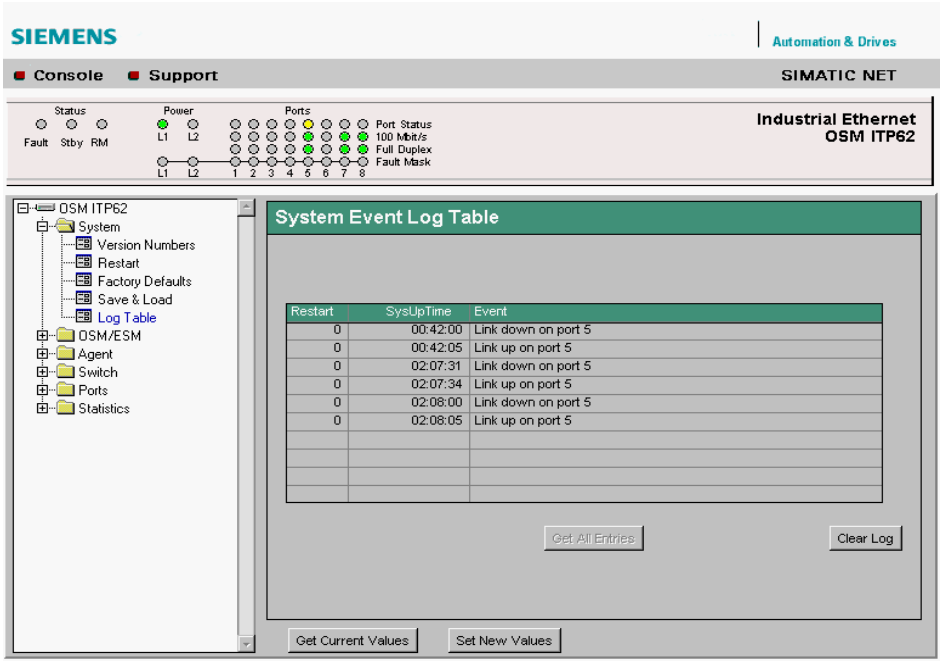


Figure 4-10 Event Log Table Window

When the window is opened the first time, the latest 30 entries in the event log table are displayed.

Click the **Get All Entries** button to display all entries in the event log table.

Click the **Clear Log** button to clear the content of the table.

4.8 OSM/ESM Status

The **OSM/ESM Status** window (Figure 4-11) shows the mode in which the OSM/ESM is operating and whether errors have been detected by the OSM/ESM.

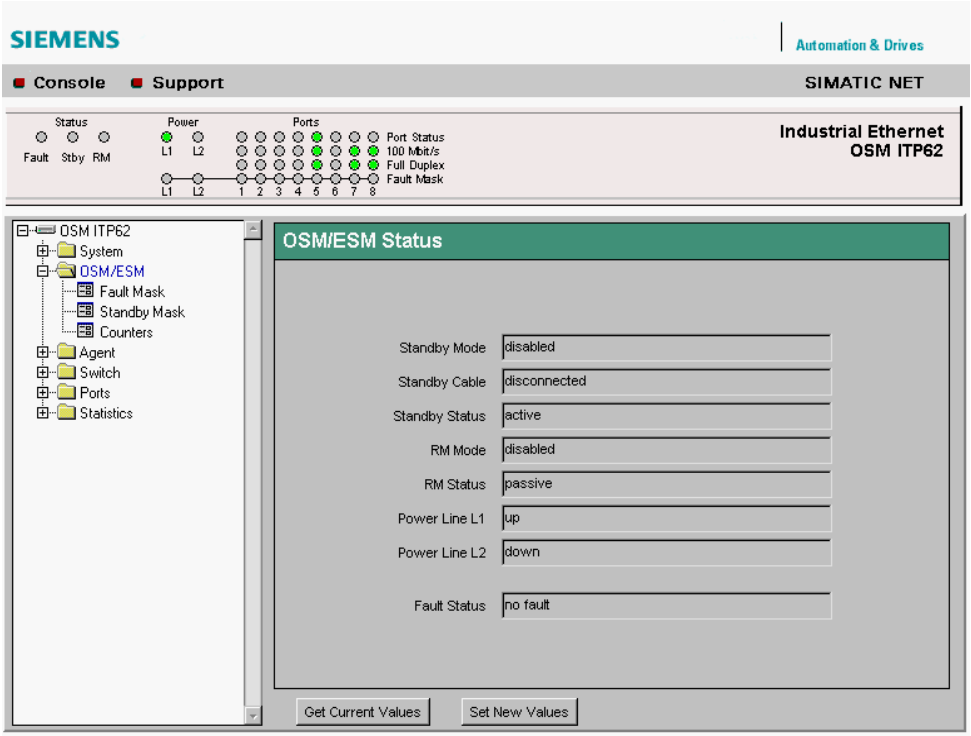


Figure 4-11 OSM/ESM Status Window

Standby Mode

Enabled:
Shows that the OSM/ESM was switched to the standby mode with the DIP switch, see /1/.

Disabled:
The standby mode is not active (DIP switch on the OSM/ESM set to “Stby off”).

Standby Cable

Connected:
The standby cable (ITP-XP standard cable 9/9) is connected to the OSM/ESM.

Disconnected:
The standby cable (ITP-XP standard cable 9/9) is not connected to the OSM/ESM or is interrupted.

Standby Status

Passive:
The OSM/ESM is passive; in other words, it does not pass on any packets via the standby ports.

Active:
The OSM/ESM is active; in other words, it passes on packets via the standby ports.

RM Mode

Disabled:
The OSM/ESM is not operating as the redundancy manager (RM).

Enabled:
The OSM/ESM is operating as the redundancy manager (DIP switch set to “RM on”).

RM Status

Passive:
The OSM/ESM is operating as the redundancy manager and has opened the ring; in other words, the line of OSMs/ESMs attached to it (ports 7 and 8) is operating without problems. The passive status is also indicated when the RM mode is disabled.

Active:
The OSM/ESM is operating as the redundancy manager and has closed the ring; in other words, the line of OSMs/ESMs attached to it (ports 7 and 8) is interrupted (fault or error). The redundancy manager switches the link between ports 7 and 8 through and reestablishes a functioning bus configuration.

Power Line 1

Up:	Power supply 1 (line 1) is applied.
Down:	Power supply 1 is not applied or has a value less than 14 V.

Power Line 2

Up:	Power supply 2 (line 2) is applied.
Down:	Power supply 2 is not applied or has a value less than 18 V.

Fault Status

Redundant power line down:

Link down on monitored port:

Standby configuration error:

More than one RM in ring:

STBY DIP switch changed. Please restart!:
The standby DIP switch setting was changed. As a result, the current operating state is inconsistent with the device configuration. The modified device configuration is adopted only after a restart.

RM DIP switch changed. Please restart!: As a result, the current operating state is inconsistent with the device configuration. The modified device configuration is adopted only after a restart.

Port x in partition mode:

Observer detected error:
Observer error.

Non-recoverable ring error:

Factory Defaults, please restart: As a result, the current operating state is inconsistent with the device configuration. The modified device configuration is adopted only after a restart.

No Fault:
The OSM/ESM has not detected a fault, the signaling contact and fault LED have not responded.

4.8.1 OSM/ESM Fault Mask

Figure 4-12 shows the **Fault Mask** window.

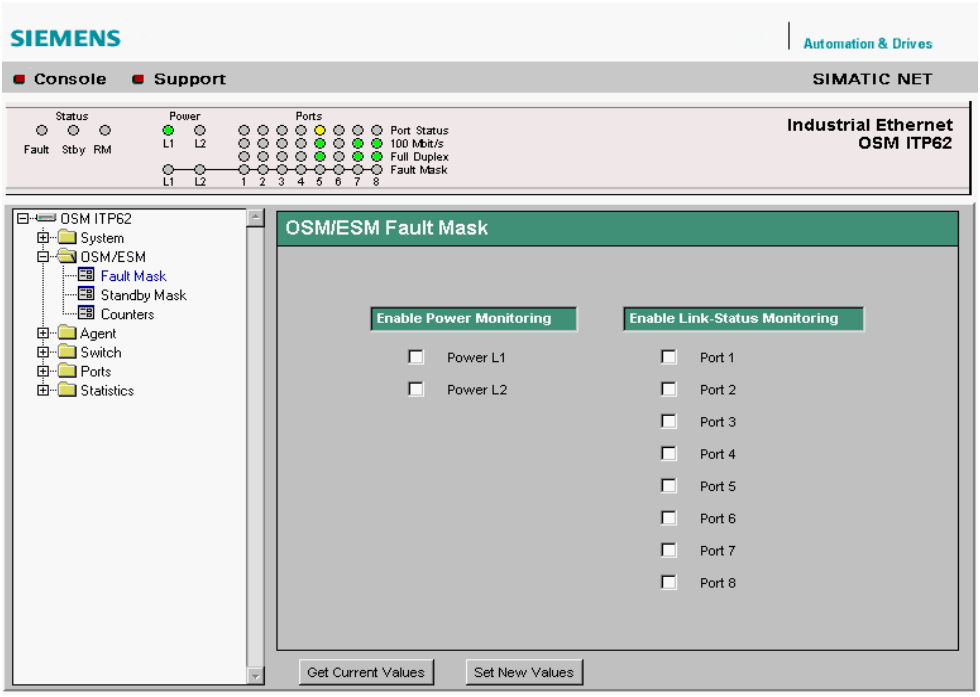


Figure 4-12 OSM/ESM Fault Mask Window

The fault mask is used to specify which fault states are monitored by the OSM/ESM and lead to the signaling contact being triggered and the fault LED being lit.

The fault mask can also be set using the buttons on the front panel of the OSM/ESM, see /1/.

Enable Power Monitoring

This specifies which of the two power supply lines 1 and 2 is monitored. A fault is indicated by the signaling contact when there is no power on one of the monitored lines (line 1 or line 2) or when the voltage is too low (less than 14 V).

Enable Link Status Monitoring

This enables/disables the link monitoring for ports 1 to 4 or 1 to 8. If the monitoring is activated on one of the ports, a fault is signaled (fault LED, signaling contact) when there is no valid link at this port (for example cable not plugged in or connected device turned off).

Set New Values

To change the settings in the fault mask, follow the steps outlined below:

1. Click the check box in the fault mask to decide which of the power supplies and ports will be monitored.
2. Then click the **Set New Values** button.

Note

Fault Mask and RM Mode

Activating the RM mode means that the ring ports (ports 7, 8) are entered in the fault mask. Deactivating the RM mode alone, does not mean that the ring ports are taken out of the fault mask. To do this, the fault mask must be reconfigured.

4.8.2 OSM/ESM Standby Mask

Clicking the **Standby Mask** menu opens the window shown in Figure 4-13 .

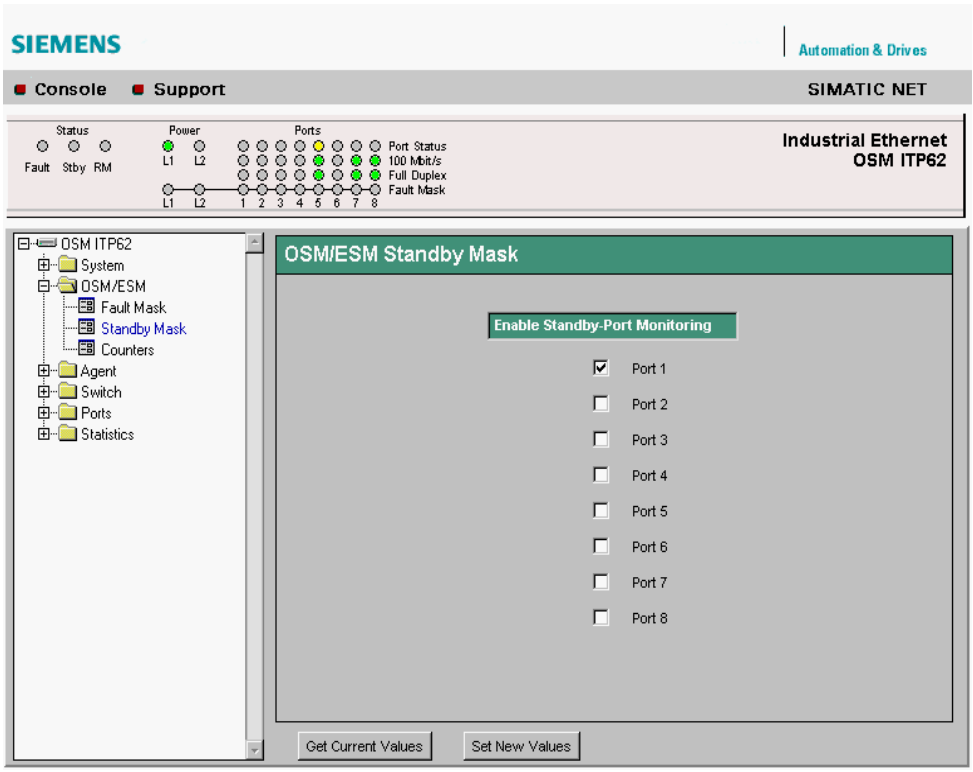


Figure 4-13 OSM/ESM Standby Mask Window

With network management, you can define several standby ports when rings are coupled redundantly, see Section 2.16. With a redundant configuration, you can then interconnect several rings or networks redundantly.

In the standby mask, you specify which ports of the OSM/ESM will operate as standby ports when working in the standby mode.

If there is no fault, only the standby ports of the standby master are active and handle the data exchange. If the standby master or the link of one of the standby ports of the master fails, **all** standby ports of the master are disabled and the standby ports of the slave activated so that a functioning configuration is established.

Please remember that the same ports on the standby master and on the standby slave must be configured as the standby ports. If an optical port of the OSM ITP62 is used in the extended redundant configuration, it must have a hardware version of at least 2.

To modify the assignments in the standby mask, follow the steps outlined below:

1. Select the ports to be monitored by clicking the relevant check boxes in the mask.
2. Then click the **Set New Values** button.

4.8.3 OSM/ESM Counters

Figure 4-14 shows the **OSM/ESM Counters** window. Using the OSM/ESM counters, you can monitor whether and how often problems occurred during operation (for example how often the signaling contact responded). The fault counters are cleared when the power supply to the OSM/ESM is turned off or when you click the **Reset Counters** button in the window.

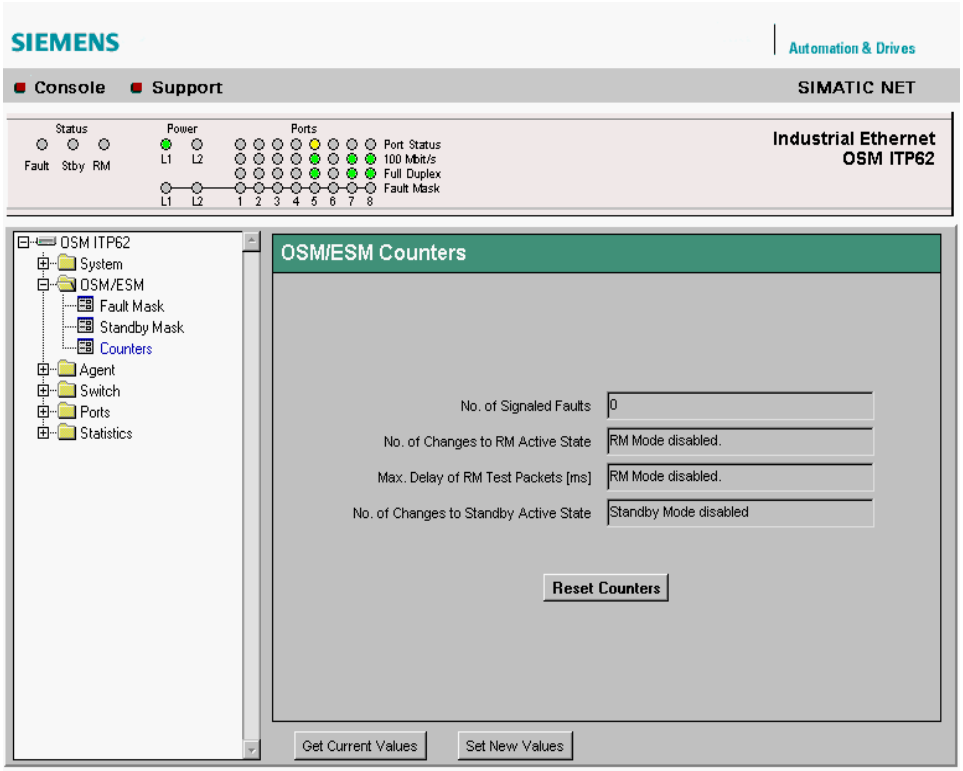


Figure 4-14 OSM/ESM Counters Window

No. of Signaled Faults

This indicates how often the signaling contact of the OSM/ESM responded.

No. of Changes to RM Active State

(Only in the redundancy manager mode) This indicates how often the OSM/ESM acting as the redundancy manager changed to the active state. This state is adopted only when the RM has detected a break on the line of OSMs/ESMs connected to the ring ports (port 7 and 8 of 8-port devices, port 3 and 4 of 4-port devices). If the RM mode is disabled (DIP switch RM “off”), no value is displayed.

Maximum Delay of RM Test Packets (ms)

This display is only active in the redundancy manager mode (RM “on”). In the redundancy manager mode, the OSM/ESM sends test packets on the line of OSMs/ESMs attached to ports 7 and 8 and measures the round-trip time of the test packets. The maximum delay of the test packets that occurs is displayed. This value should not exceed 50 ms.

No. of Changes to Standby Active State

This counter is only active when the standby mode was activated with the DIP switch on the OSM/ESM (”Stby on”). It indicates how often the OSM/ESM acting as the standby slave switched to the active mode in the redundant configuration. (This can be caused by failure of the standby master or because there was no longer a valid link at a standby port of the standby master.)

4.9 Agent Features

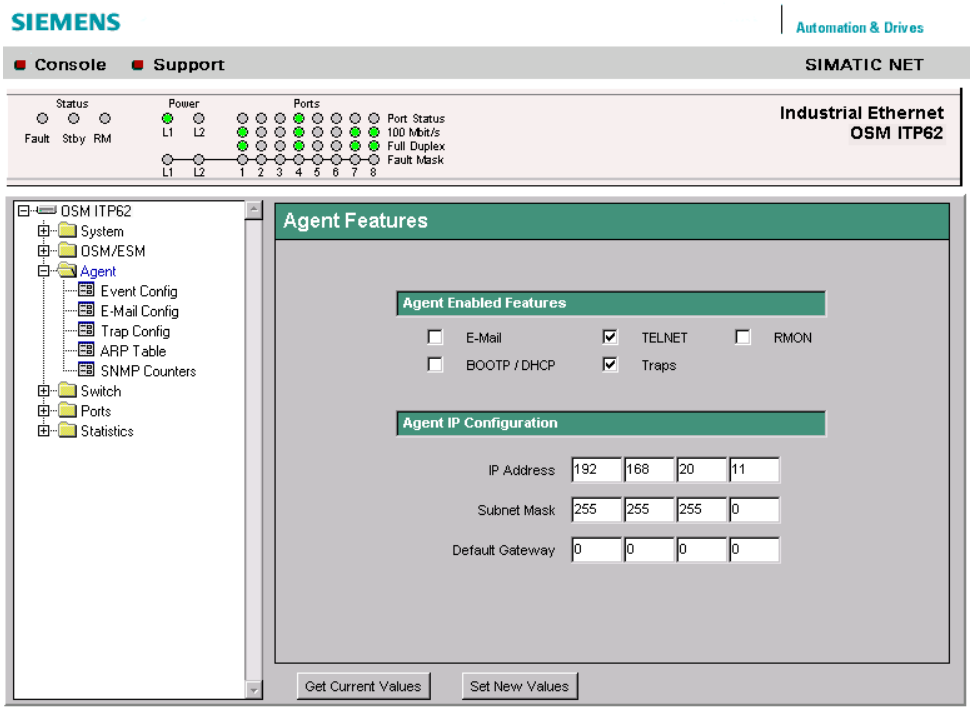


Figure 4-15 Agent Window

E-Mail

This is used to enable or disable the E-mail function of the OSM/ESM, see Section 2.9.

TELNET

This enables or disables TELNET access, see Section 2.14.

RMON

This enables or disables Remote Monitoring (RMON), see Section 5.

RMON is available on all OSMs/ESMs except for the OSM TP22 and the ESM TP40.

BOOTP/DHCP

BOOTP/DHCP specifies whether BOOTP/DHCP is active for the OSM/ESM, see Section 2.13.

Traps

The traps check box is used to enable or disable the issuing of traps, see Section 2.8

IP Address

IP address of the OSM/ESM.

Note

If the IP address of the OSM/ESM is changed, the browser link to the OSM/ESM is lost. Close the OSM/ESM window in the Internet browser and reconnect to the OSM/ESM with the new IP address.

Subnet Mask

Subnet mask of the OSM/ESM.

Default Gateway

Default gateway displays the IP address of the default gateway. (This must be entered if the PC/Internet browser is not located in the same subnet as the OSM/ESM.)

Set New Values

To change the entries in this window, follow the steps outlined below:

1. Click the check boxes to decide which functions are enabled and disabled.
2. If necessary, update the IP address, subnet mask or address of the default gateway.
3. Then click the **Set New Values** button.

4.9.1 Agent Event Configuration

In the Agent Event Configuration window (Figure 4-16), you can select the specific action (E-mail, trap, or entry in the event log table) triggered for each event.

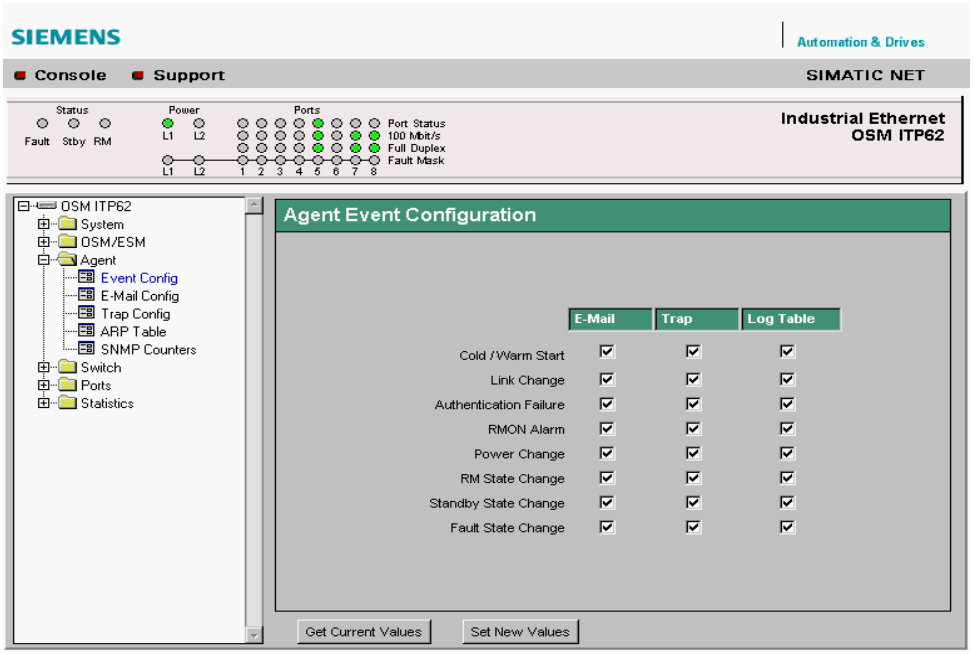


Figure 4-16 Agent Event Configuration Window

4.9.2 Digital Input Configuration (only OSMs/ESMs with digital inputs)

You can change the configuration of the digital inputs in the Digital Input Configuration window (Figure 4-17).

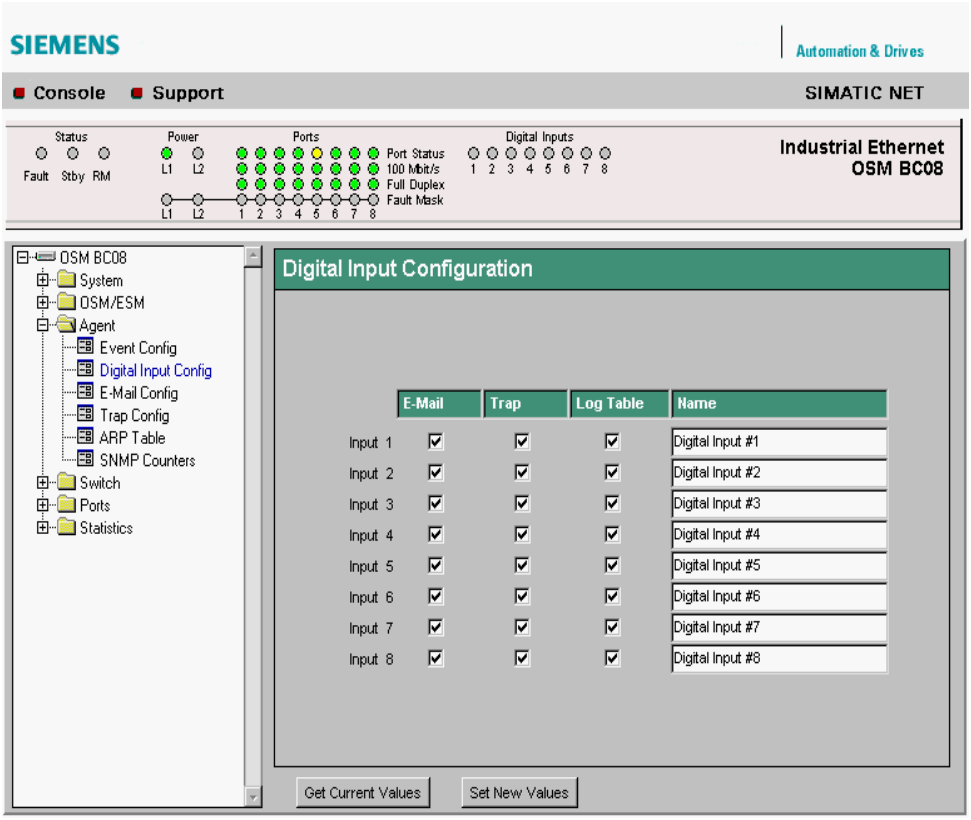


Figure 4-17 Digital Input Configuration Window

You can specify specific events such as E-mail, trap, and entry in the log table for each input. You can enter the name of the digital input in the **Name** box.

4.9.3 Agent E-Mail Configuration

Figure 4-18 shows the **Agent E-Mail Configuration** window.

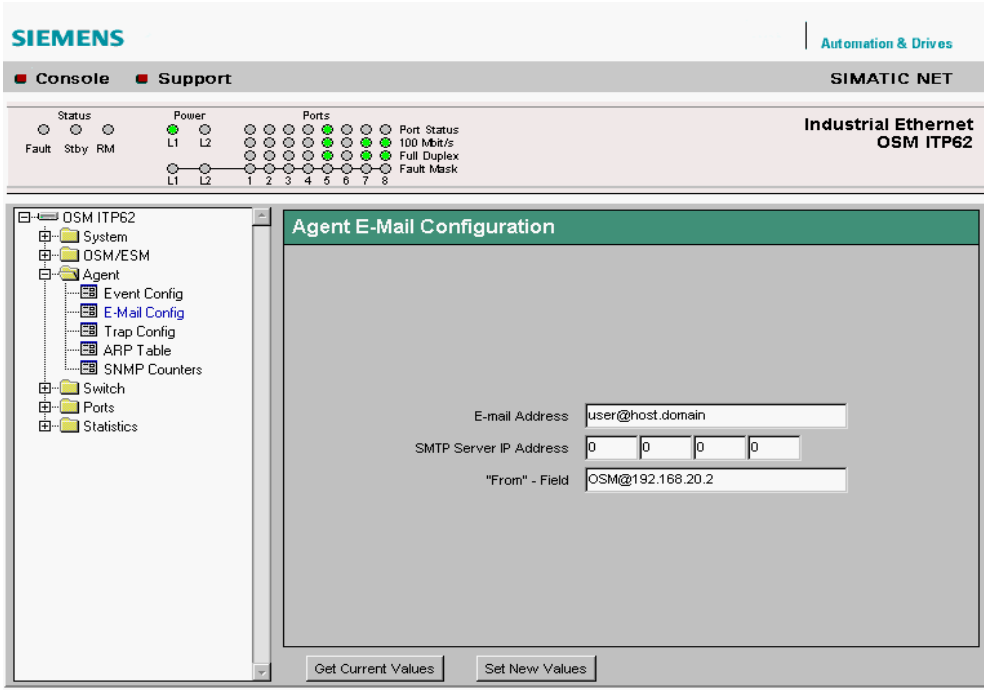


Figure 4-18 Agent E-Mail Configuration Window

When certain faults occur and are detected by the OSM/ESM, it can automatically send an E-mail to a selected E-mail address containing an error message in plain language, see Section 2.9. Before an E-mail can be sent, it must be configured in this window and be activated in the “Agent Menu”, see Section 4.9.

E-Mail Address

Enter the E-mail address to which the E-mail will be sent if faults occur.

SMTP Server IP Address

Here, you enter the IP address of the SMTP server via which the E-mail will be sent. Make sure that the OSM/ESM can access the SMTP server.

“From” Field

Address of the sender of the E-mails. Depending on the type and configuration of the SMTP server it may be necessary to configure the sender address. If no entry is made, the OSM/ESM uses the following address:
OSM@<IP - address>
or
ESM@<IP - address>

Set New Values

To set an E-mail address and the IP address of the SMTP server, follow the steps outlined below:

1. Enter the E-mail address and IP address of the SMTP server in the boxes.
2. Then click the **Set New Values** button.

4.9.4 Agent Trap Configuration

Clicking the **Trap Config** menu opens the window shown in Figure 4-19.

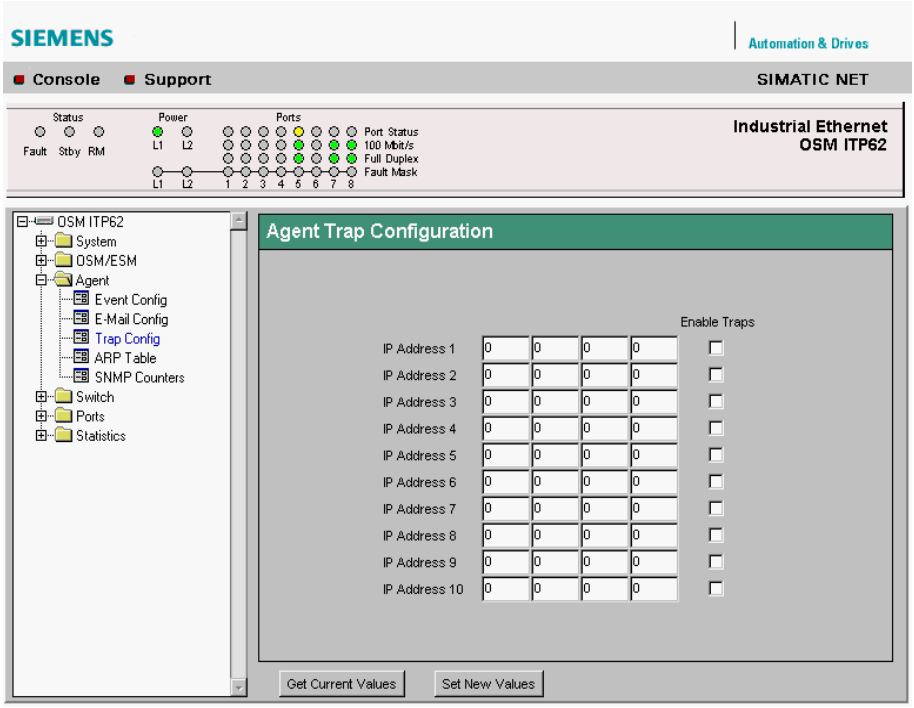


Figure 4-19 Agent Trap Configuration Window

If an alarm occurs, the OSM/ESM can send traps (alarm messages) to up to 10 different (network management) stations at the same time, see Section 2.8. In this menu, you enter the addresses of the stations to which the traps will be sent. Follow the steps outlined below:

Set New Values

1. Enter the IP addresses of the stations to which the traps will be sent.
2. Click the check boxes beside the IP addresses to activate the sending of traps to these stations.

Then click the **Set New Values** button.

4.9.5 Agent ARP Table

Clicking the **ARP Table** menu opens the window shown in Figure 4-20.

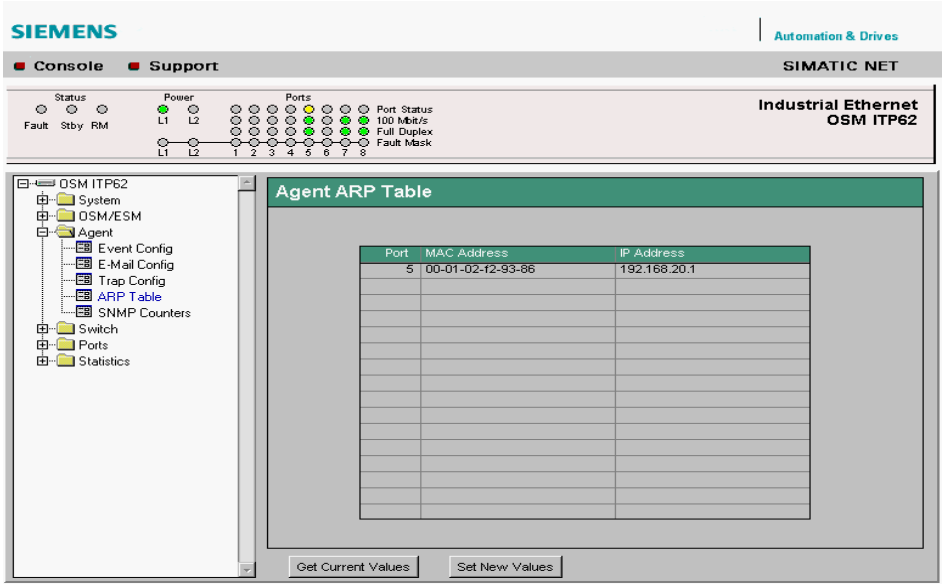


Figure 4-20 Agent ARP Table Window

The Agent ARP Table (ARP cache) displays the MAC and IP addresses of the stations that exchange information with OSM/ESM Network Management. This means all stations that communicate with the OSM/ESM using SNMP, WBM, TELNET. The entry in the ARP table is only cleared when the corresponding station has not exchanged any data with the OSM/ESM for more than fifteen minutes.

4.9.6 Agent SNMP Counters

The Agent **SNMP Counters** window (Figure 4-21) displays counter values defined in the SNMP standard RFC 1213 (MIB-II). The meaning of these counter values is described in RFC 1213. Interpreting the counter values requires detailed knowledge of RFC 1213. The counters can be used, for example, to provide diagnostic information about problems occurring on the link to the SNMP management station.

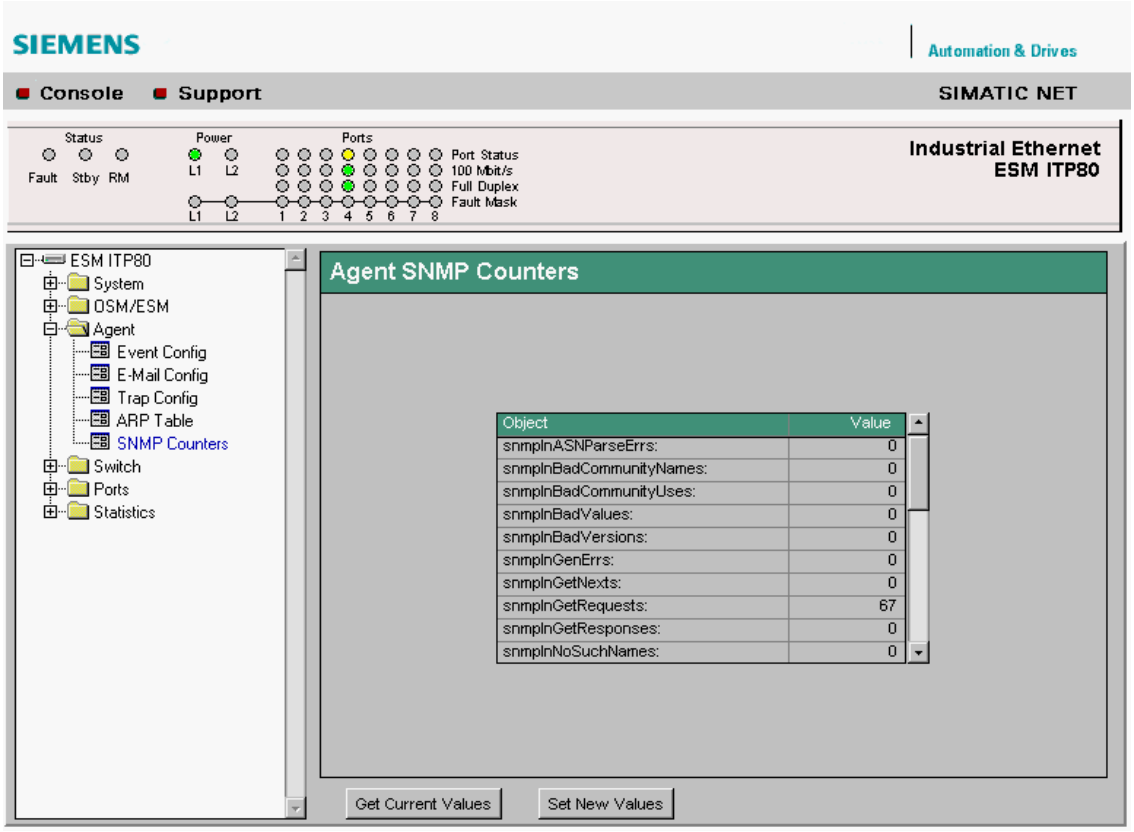


Figure 4-21 Agent SNMP Counters Window

Object

This column contains the names of the SNMP counter objects.

Value

This displays the current counter values.

4.10 Switch Features

Figure 4-22 shows the **Switch** window.

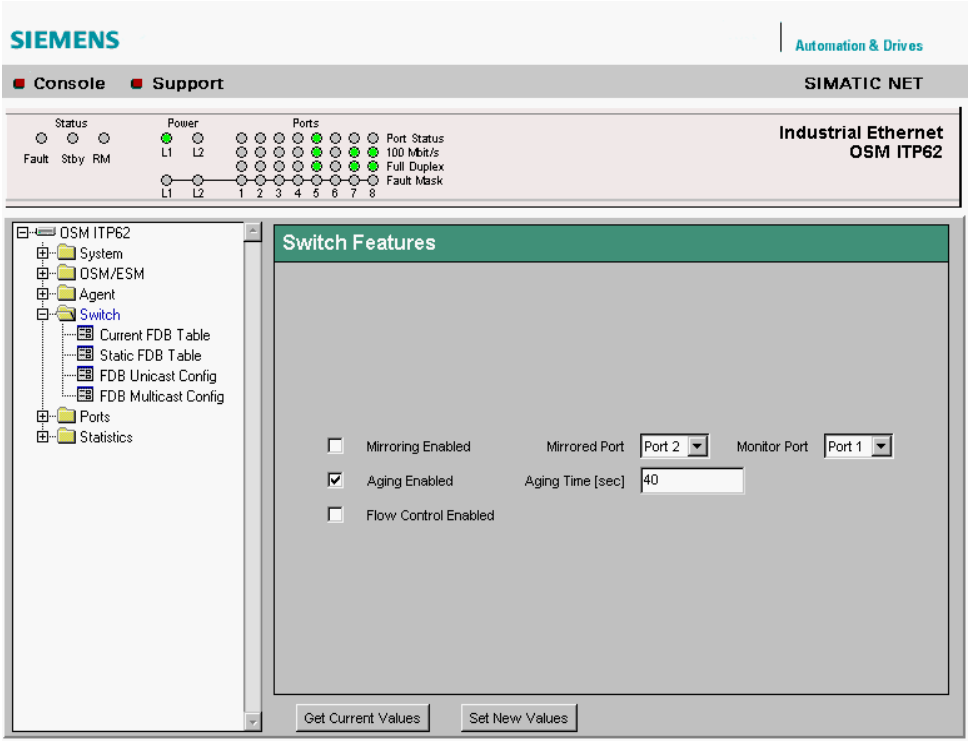


Figure 4-22 Switch Features Window

Mirroring

Mirroring means that the data exchange at a port (mirrored port) of this OSM/ESM can be “reflected” to another port (monitor port). If a protocol analyzer is connected to the monitor port, it can be used to record the data exchange at the mirrored port without interrupting the connection at the mirrored port. To use this function, there must be a free port on the OSM/ESM that can be used as the monitor port.

Aging

OSMs/ESMs automatically learn the source addresses of the nodes connected to them. This information is used on the OSM/ESM to pass packets to the intended recipients. This reduces the network load for the other nodes.

If the OSM/ESM does not receive a packet with a source address that matches a learned address within the aging time, it deletes the address from the database. This prevents packets being passed on incorrectly if, for example, a DTE is connected to a different OSM/ESM port. The default for the aging time is 40 seconds. By setting aging to disabled, addresses are no longer automatically deleted.

Flow Control

Using flow control, the OSM/ESM can slow down the reception of further packets at the ports if the network is overloaded. Flow control must be activated separately for the individual ports in the port mask. If the Flow Control Enable check box is deactivated in the Switch window, the flow control mechanism is deactivated for all ports regardless of the settings made in the port masks.

Set New Value

Follow the steps outlined below to change settings in the Switch window:

1. First, enable the check box for the individual parameters by clicking them or select the **mirrored port** or **monitor port** from the list boxes.
2. Then click the **Set New Values** button to enter the values.

4.10.1 Current FDB Table

Clicking the **Current FDB Table** menu opens the window with the FDB table of the OSM/ESM shown in Figure 4-23. The FDB table shows which node addresses (MAC addresses) the OSM/ESM has learned and the port on the OSM/ESM via which the node can be reached. The MAC addresses entered as static information by the user are also displayed (see Section 2.4).

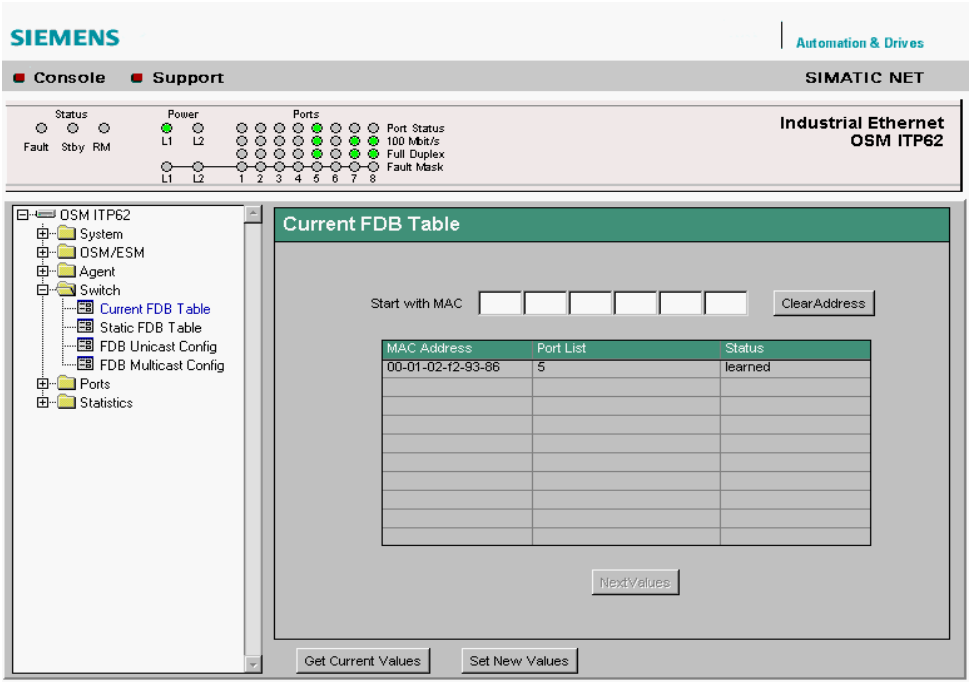


Figure 4-23 Current FDB Table Window

MAC Address

This displays the MAC address of the attached node that the OSM/ESM has learned on the basis of received packets.

Port List

This shows the ports via which the node with the specified address can be reached. Packets received by the OSM/ESM with a destination address matching this address are passed on by the OSM/ESM to this port. With multicast addresses, the port list shows the OSM/ESM ports to which a received multicast packet is passed.

Status

Shows the status of each FDB entry.

”learned” means that the specified address was learned as a result of receiving a packet from this node.

”static” means that the address was entered as a static address by the user. Static addresses are stored permanently; in other words, they are not cleared after the aging time has elapsed or when the OSM/ESM is restarted.

Start with MAC

This box specifies the address from which the display of MAC addresses in the FDB table will be displayed. If nothing is entered here, the display begins at the lowest stored address.

Clear Address

This button clears the entry in the **Start with MAC** box.

Next Values

10 MAC addresses are displayed at one time. The “Next Values” button displays the next 10 addresses from the FDB table. By repeatedly clicking “Next Values” you can work through the entire FDB table.

4.10.2 Static FDB Table

Clicking the **Static FDB Table** menu opens the window shown in Figure 4-24. This window displays only the static addresses; in other words, the addresses entered by the user.

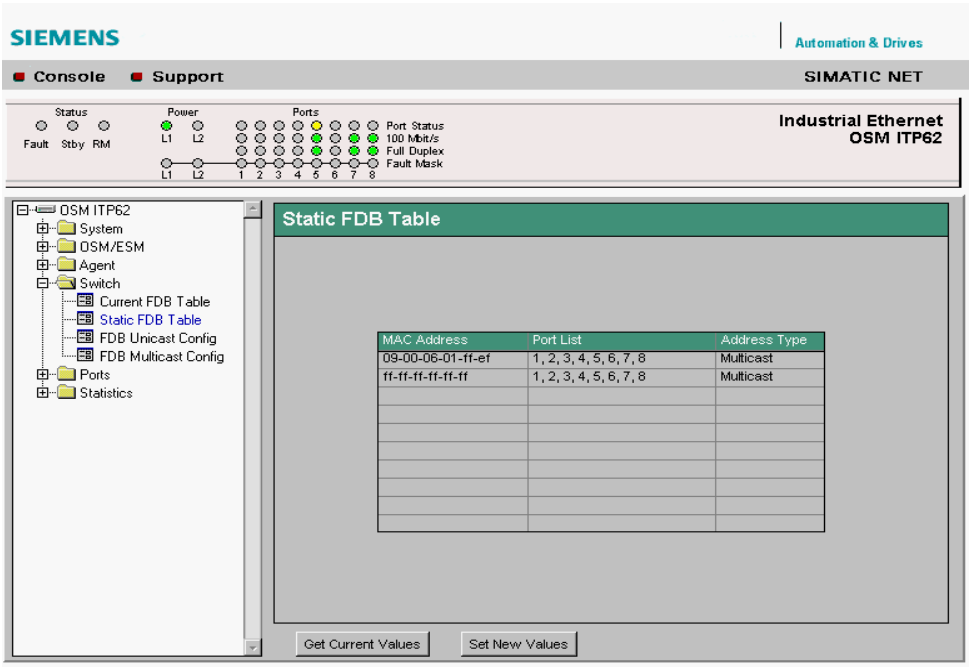


Figure 4-24 Static FDB Table Window

MAC Address

This displays the MAC address with which the MAC destination address of each incoming packet is compared to check whether the packet is rejected or passed on.

Port List

The port list shows the OSM/ESM ports to which a received packet with the entered MAC address is passed.

Address Type

The address type specifies whether the entry in the FDB table is a unicast or a multicast destination address.

4.10.3 FDB Unicast Configuration

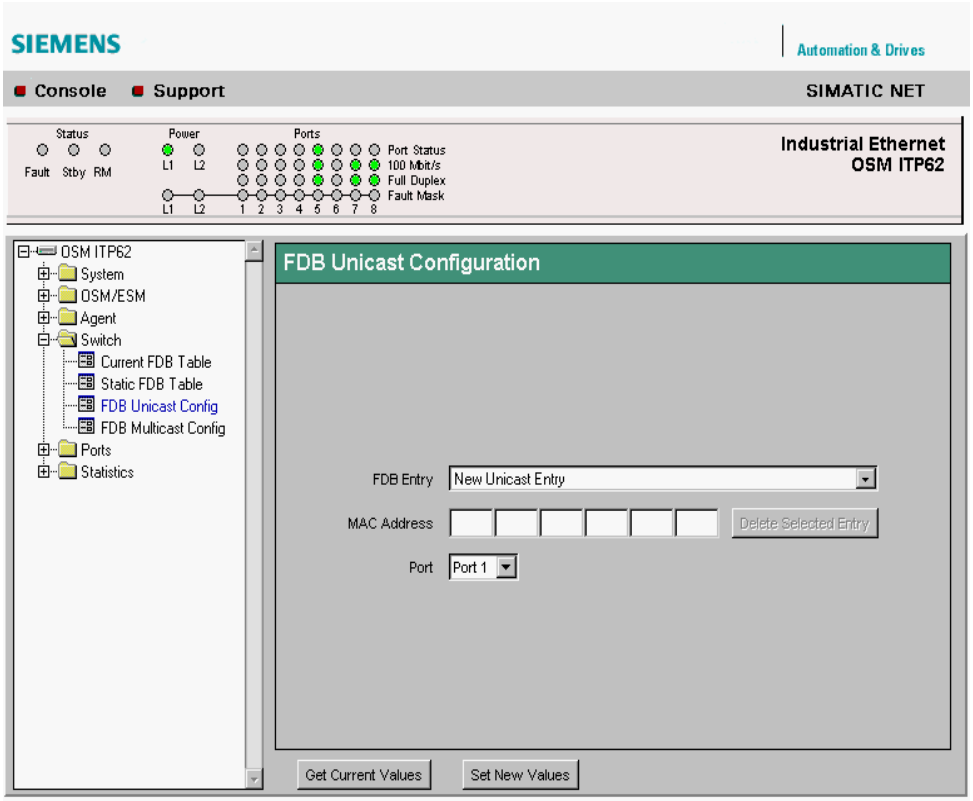


Figure 4-25 FDB Unicast Configuration Window

In this window, you can enter or clear static unicast addresses in the FDB table. Static addresses are not cleared by the address aging, see Section 2.5 and are also retained when the OSM/ESM is turned off.

Entering Static Unicast Addresses

Follow the steps outlined below:

1. Select **New Unicast Entry** in the **FDB Entry** list box.
2. Enter the MAC address in the address box in hexadecimal (in each case 1 or 2 digits in one of the 6 fields).
3. In the **Port** list box, select the port to which packets with this (destination) MAC address will be passed on.
4. Then click the **Set New Values** button.

Deleting Static Unicast Addresses

Follow the steps outlined below:

1. Select the address you want to delete in the **FDB Entry** list box.
2. Click the **Delete Selected Entry** button.

4.10.4 FDB Multicast Configuration

Clicking the **FDB Multicast Config** menu opens the window displayed in Figure 4-26. In this window, you can enter or clear (static) multicast addresses in the FDB table.

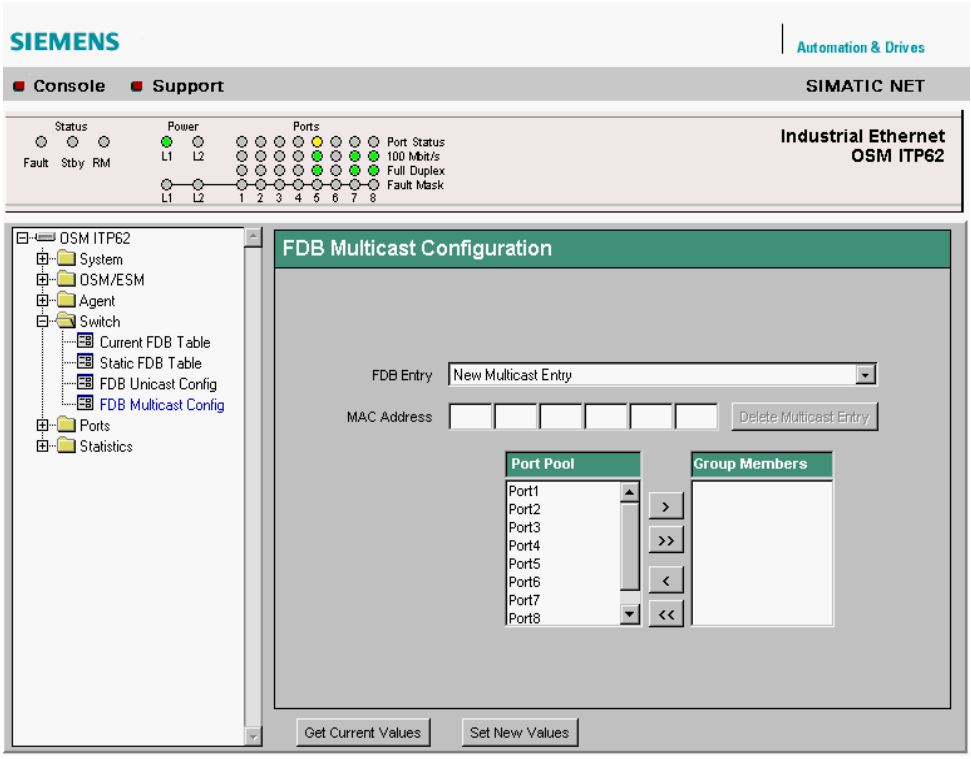


Figure 4-26 FDB Multicast Configuration Window

Entering a Multicast Address

Follow the steps outlined below to enter a multicast address in the FDB table:

1. Select **New Multicast Entry** in the **FDB Entry** list box.
2. Enter the MAC address in the box in hexadecimal. 1 or 2 digits must be entered in one of the 6 fields. If only one digit is entered, this is automatically padded with a zero.
3. You must then specify **the ports** to which a packet with the specified multicast address will be sent by the OSM/ESM. The following entries are important:

   Port Pool
   This column contains all the ports of the OSM/ESM to which multicast packets with the specified address are **not** passed on.

   Group Members
   This column contains all the ports of the OSM/ESM to which multicast packets with the specified address are passed on.

   You can move ports between the columns by clicking on the required port and then moving it with the < and > buttons. The << and >> buttons move all ports to the other column.
4. Then click the **Set New Values** button.
5. Repeat steps 1 to 4 for each MAC address for which you want to configure a “multicast” FDB entry.

Deleting a Multicast FDB Entry

Follow the steps outlined below to delete a Multicast FDB entry:

1. Select the FDB entries you want to delete in the **FDB Entry** list box.
2. Click the **Delete Multicast Entry** button.

Note

The group members specify the ports to which frames with the configured Multicast MAC address are passed. The ports via which the frames were received is unimportant. This property is also known as ingress filtering.

4.11 Port Status

Clicking the **Ports** menu opens the window shown in Figure 4-27.

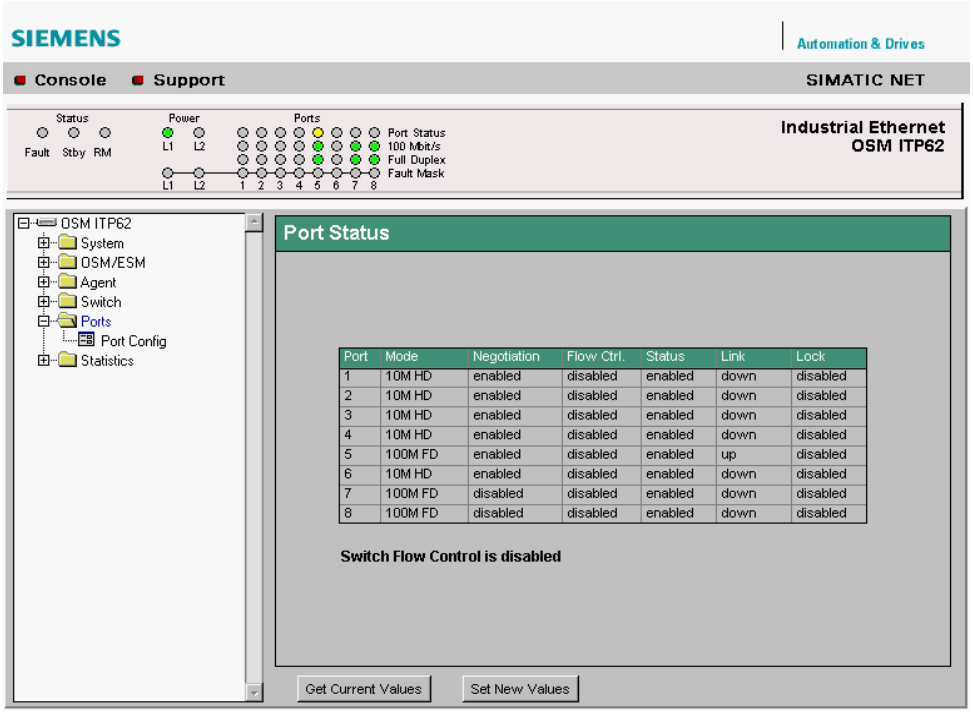


Figure 4-27 Port Status Window

Port

This contains the port number.

Mode

This indicates whether the port operates at 10 Mbps or 100 Mbps and whether it operates in the half duplex (HD) or full duplex (FD) mode.

Negotiation

This shows whether autonegotiation is set for the port.

enabled: Autonegotiation is enabled.
disabled: Autonegotiation is disabled.

Flow Ctrl

This shows whether or not flow control was activated for the port. If the port is operating in the half duplex mode, this shows whether half duplex flow control (back pressure) is active. If the port operates in the full duplex mode, this shows whether the full duplex flow control is activated.

enabled: Flow control is enabled.
disabled: Flow control is disabled.

Status

This shows whether the port is activated or deactivated. Data exchange is only possible via an activated port.

enabled: The port is activated.
disabled: The port is deactivated

Link

This shows whether the port has a valid link to the network. (For example reception of a “link integrity signal”.)

up: The port has a valid link to the network.
down: The link is interrupted
(for example connected device turned off).

Locked

This shows whether port locking is activated, see Section 2.6.

enabled:
A packet with a source address that does not exist in the FDB table of the OSM/ESM is discarded. The OSM/ESM does not learn the source address of the corresponding node.

disabled (default):
A packet with a source address that does not exist in the FDB table of the OSM/ESM is passed on by the OSM/ESM. The OSM/ESM also learns the source address of the corresponding node; in other words the MAC address is entered in the FDB table.

4.11.1 Port Configuration

In the **Port Configuration** window (Figure 4-28), you can modify the settings for the OSM/ESM ports.

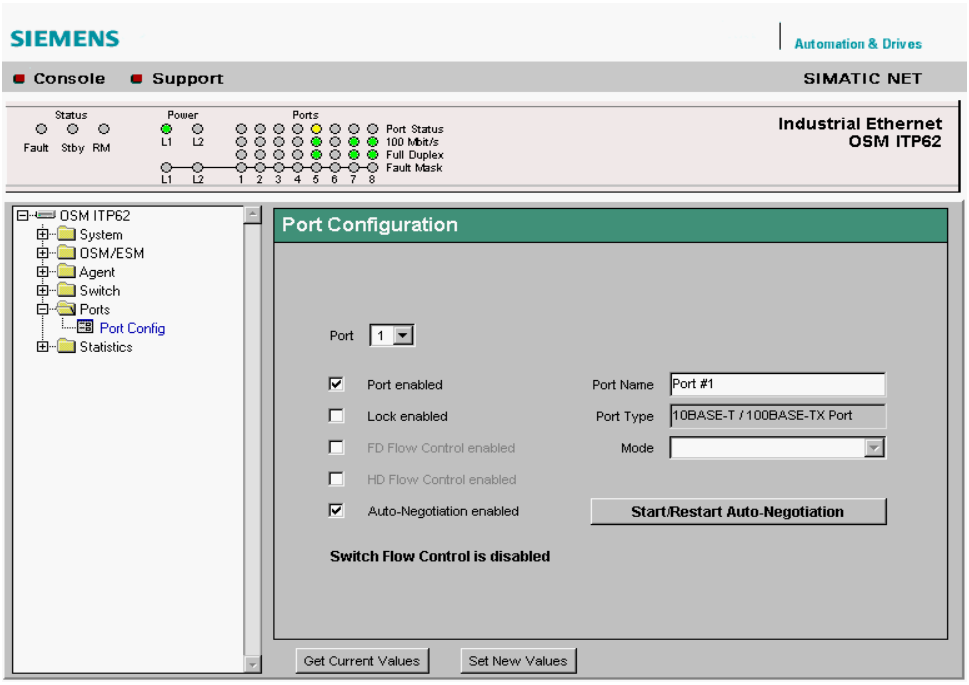


Figure 4-28 Port Configuration

Follow the steps outlined below to change the settings of a port:

1. Select the number of the required port in the **Port** list box.
2. The **Port Enabled** check box enables (✓) or disables data exchange on the port.
3. The **Lock Enabled** check box prevents (✓) or allows the passing on of packets whose source address is not in the FDB table of the OSM/ESM.
4. The **FD Flow Control Enabled** check box enables (✓) or disables full duplex flow control for a port. Full duplex flow control is only effective when the port operates in the full duplex mode.
5. The **HD Flow Control Enabled** check box enables (✓) or disables half duplex flow control. Half duplex flow control is only effective when the port is operating in the half duplex mode.
6. The **Autonegotiation Enabled** check box enables (✓) or disables autonegotiation for a port.

7. If autonegotiation is disabled, you can set the transmission rate and duplicity of the port in the **Mode** list box. If autonegotiation is active, these parameters are automatically negotiated by the OSM/ESM and the connected DTE, see Section 2.1.
8. You can enter the name of the port in the **Port Name** box.
9. Click the **Set New Values** button to enter the modified values.

Autonegotiation (the negotiation of the transmission rate and duplicity) is generally started only when a device is connected or started up. If you click the **Start/Restart Autonegotiation** button, you can start autonegotiation immediately.

Note

Do not deactivate autonegotiation if you want to use the autocrossover function with the partner port.

4.12 Statistics Counters

The OSM/ESM has internal statistical counters (RMON counters) with which the number of received packets (sorted according to length and type) and the number of bad packets for each port can be counted. This information provides you with an overview of the data traffic and any network problems that may have occurred.

Resetting the Statistics Counters

Follow the steps outlined below to reset the RMON counters to zero:

1. Click the Statistics menu to open the window shown in Figure 4-29.
2. Click the **Reset Statistics Counters** button.

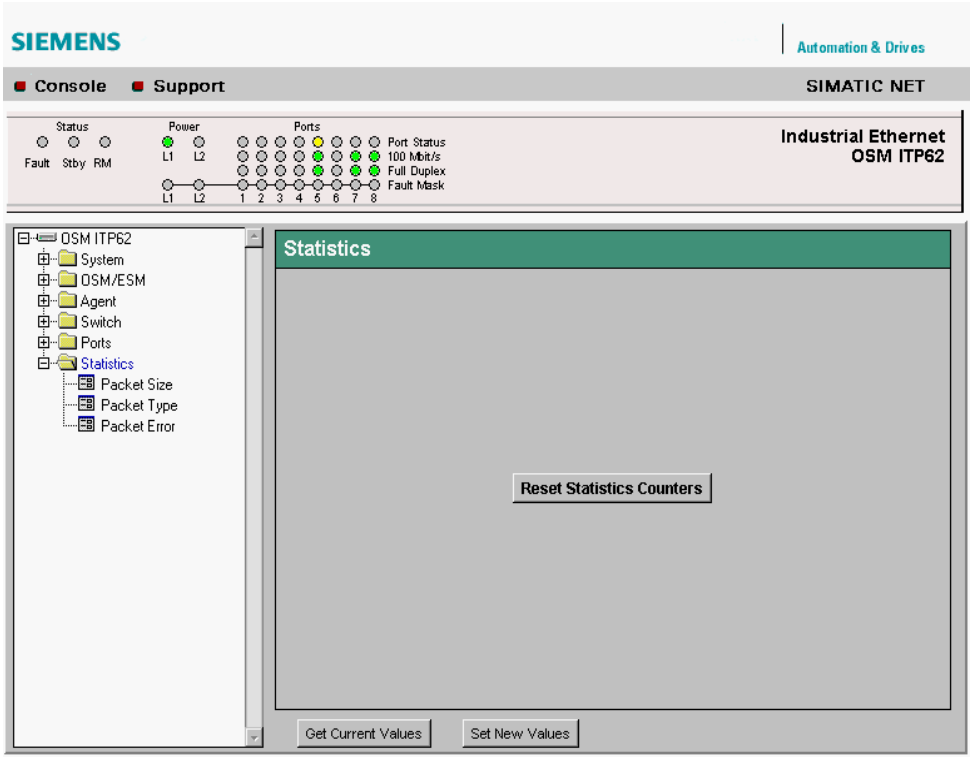


Figure 4-29 Statistics

4.12.1 Packet Size

The Packet Size window displays the number of packets received at a port arranged according to the packet size. The following packet sizes are displayed: 64, 65-127, 128-255, 256-511, 512-1023 and 1024-1536 bytes.

Follow the steps outlined below to read out the packet counter:

1. Click the Packet Size window to open the window shown in Figure 4-30.
2. Select the port you want to view in the Port list box.
3. Select the packet sizes you want to have displayed.
4. Click the **Get Current Values** button.
   The number of packets in each range and a pie chart is displayed providing you with an overview of the distribution of packet sizes (see Figure 4-30).
   If no packet with the selected sizes was received, no pie chart is displayed.

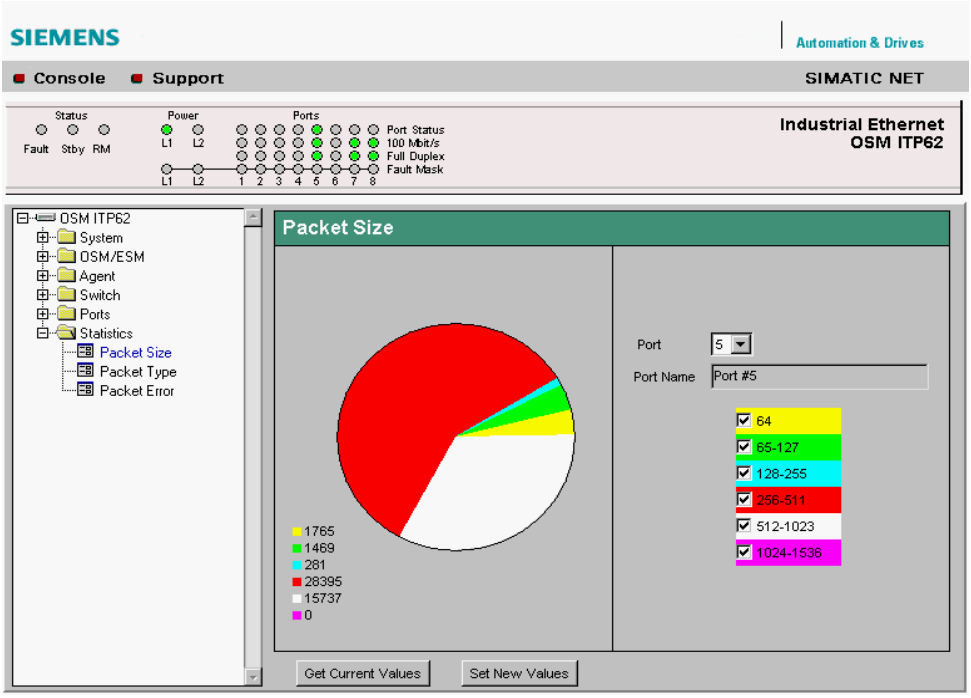


Figure 4-30 Packet Size Window

4.12.2 Packet Type

This window displays the packets of each port according to three types or classes: unicast, multicast and broadcast packets, refer to the Glossary, Appendix F.

Follow the steps outlined below to display the “Packet Type” counters (Figure 4-31):

1. Select the port you want to view in the Port list box.
2. Select the packet types (unicast, multicast, broadcast) you want to have displayed.
3. Click the **Get Current Values** button.
   The number of packets of each type is displayed along with a pie chart that provides you with an overview of the distribution of packet types, see Figure 4-31. (If no packets of the selected types were received, no pie chart is displayed.)

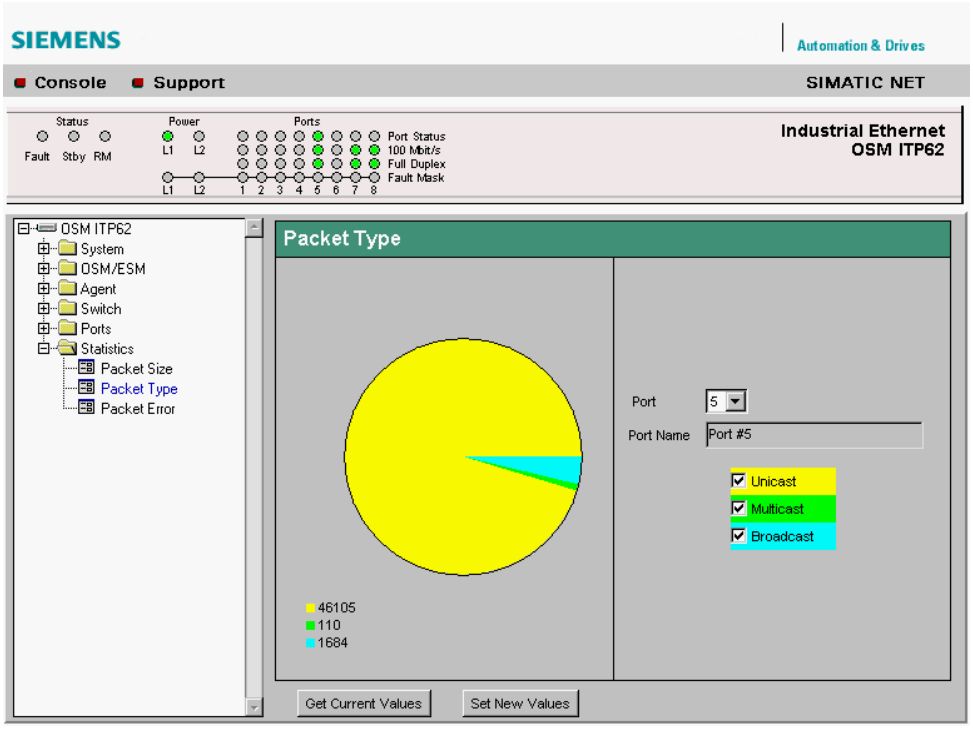


Figure 4-31 Packet Type

4.12.3 Packet Error

For each port, the OSM/ESM can detect the following errors in received packets and display the errors with the following counters: CRC, Undersize, Oversize, Jabbers and Collisions, see Glossary.

Follow the steps outlined below to display the bad packets counted for a port of the OSM/ESM:

1. Select the **Packet Error** menu (Figure 4-32).
2. Select the port you want to view in the Port list box.
3. Select the packet errors you want to have displayed: CRC, Undersize, Oversize, Jabbers, or Collisions.
4. Click the **Get Current Values** button.
   The number of packets in each error class along with a bar diagram is displayed, see Figure 4-32. (If there are no packets in the selected classes, no bar diagram is displayed.)

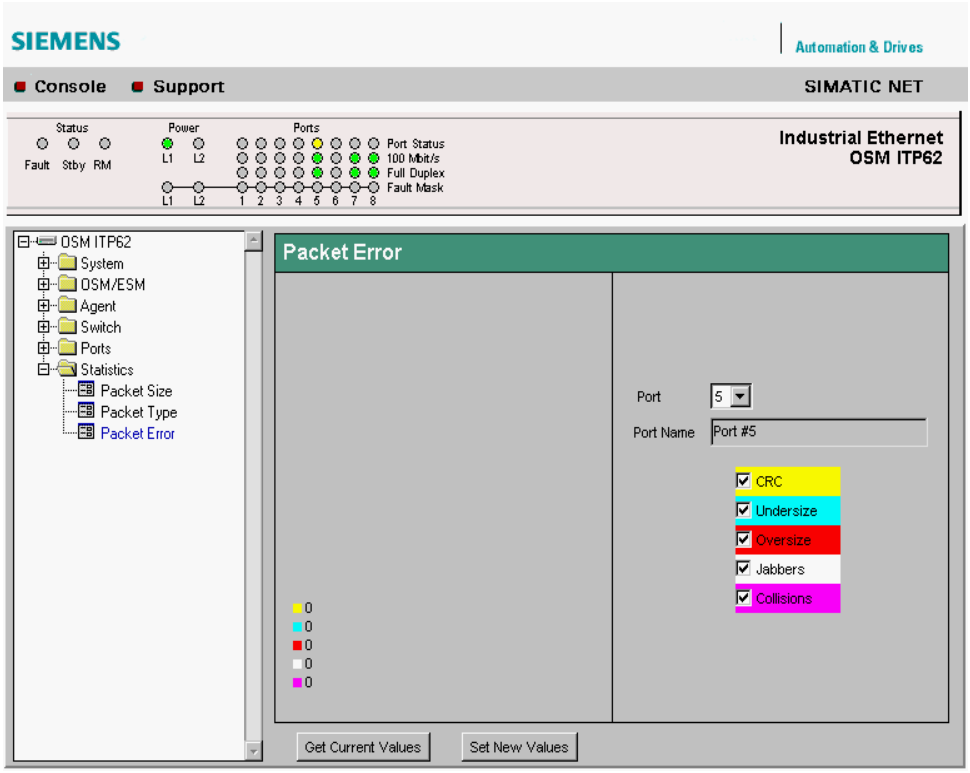


Figure 4-32 Packet Error Window

SNMP and RMON

5

5.1 SNMP

With SNMP (Simple Network Management Protocol), a network management station can configure and monitor SNMP-compliant nodes such as the OSM/ESM (from firmware Version 2.0 and higher). To make this possible, a management agent is installed in the DTE with which the management station exchanges data using SNMP Get and Set requests. The OSMs/ESMs support SNMP V1.

The data that can be managed are in a database on the OSM/ESM (DTE) known as the MIB (**M**anagement **I**nformation **B**ase) that can be accessed by the management station (or the applet of the OSM/ESM Web-Based Management) using the agent.

There are standardized MIBs defined in RFCs and private MIBs containing product-specific extensions that are not covered in standard MIBs.

The OSMs/ESMs with network management support the following MIBs:

- RFC 1213: MIB II
- RFC 2233: Interface MIB
- RFC 1286, RFC1493: Bridge MIB
- RFC 1757: RMON MIB

OSM/ESM private MIB

The private MIB of the OSM/ESM is on the supplied CD. The private MIB file can also be downloaded from an OSM/ESM directly with a Web browser at http://<IP address of the OSM/ESM>/snOSM.mib. Please note the capitalization of snOSM.mib! In the Internet Explorer, click on View and save the MIB as source text. The description of the MIB objects of the private MIB is included in the MIB and can be read directly with a MIB compiler (for example the network management station) or with a text editor.

The **read-only community string** (SNMP password for read access) is set to **public**, the **read-write community string** (SNMP password for read and write access) is set to **private** and can be changed using SNMP or the Agent menu in the CLI, see Section 3.5.

5.2 RMON

A RMON-compliant device (RMON = **R**emote **MON**itoring) allows you to collect special diagnostic data on the device, to prepare this data and to read it out via SNMP at a network management station that supports RMON. This diagnostic data such as port-related load allows you to detect network problems early and to eliminate them. These are stored on the OSM/ESM in the RMON MIB.

RMON functionality is defined in RFC 1757 and is divided into groups. All OSMs/ESMs with the exception of OSM TP22 and ESM TP40 support the four RMON groups Statistics, History, Alarm and Event.

The following table summarizes the options provided by these four groups.

Table 5-1 RMON Groups and Their Functionality

RMON Group	Description
Statistics	This provides statistical information for each OSM/ESM port such as packet rate, packet distribution, number of broadcast, multicast, unicast packets, number of received bad packets sorted according to error types.
History	This RMON group allows specific statistical information on the OSM/ESM to be selected, queried at periodic intervals and stored. You can read out this information at a management station later and display it in chronological order (for example the chronological order of the error rate).
Alarm	The alarm group also queries certain statistical values periodically and compares them with limit values configured previously on the OSM/ESM by the management station. If a limit value is violated, an alarm is generated and a trap is issued. The alarm group is only possible when the event group is supported.
Event	The event group controls generation of traps when RMON alarms occur.

6 Upgrading/Downloading Software

6.1 General Introduction

The firmware of the OSM/ESM can be loaded in two different ways:

- Over the serial port of the OSM/ESM
- From a TFTP server, see also Section 6.3.

You will find information on firmware updates for OSM/ESM on the Web at http://www.ad.siemens.de/csi/net.

This chapter describes the downloading of the OSM/ESM firmware in detail.

Note

After you have downloaded the firmware, the new firmware is stored in non-volatile memory on the OSM/ESM and the original firmware is erased. If the power supply to the OSM/ESM is interrupted during the download, the loaded firmware may be incomplete and not executable. You can recognize this by the fault LED being lit permanently and when the display LEDs do not switch over when you press the OSM/ESM button (after the OSM/ESM has started up). In this case, the firmware must be downloaded again via the serial port, see Section 6.2. It is then no longer possible to download the firmware from a TFTP server.

6.2 Downloading the Firmware via the Serial Port

To download the firmware via a serial port of the OSM/ESM, follow the steps outlined below:

1. Connect a PC with the Hyperterminal program as described in Appendix B and start Hyperterminal.
2. Reset the OSM/ESM by pressing the Select/Set button during operation (if necessary several times briefly) until the display LEDs display the port status (all display LEDs off). Then press the Select/Set button for at least 6 seconds. After approximately 3 seconds, the display LEDs start to flash, after a further 2 seconds the reset is executed (all LEDs go on briefly and then off again).

The following message then appears in the terminal window of Hyperterminal:

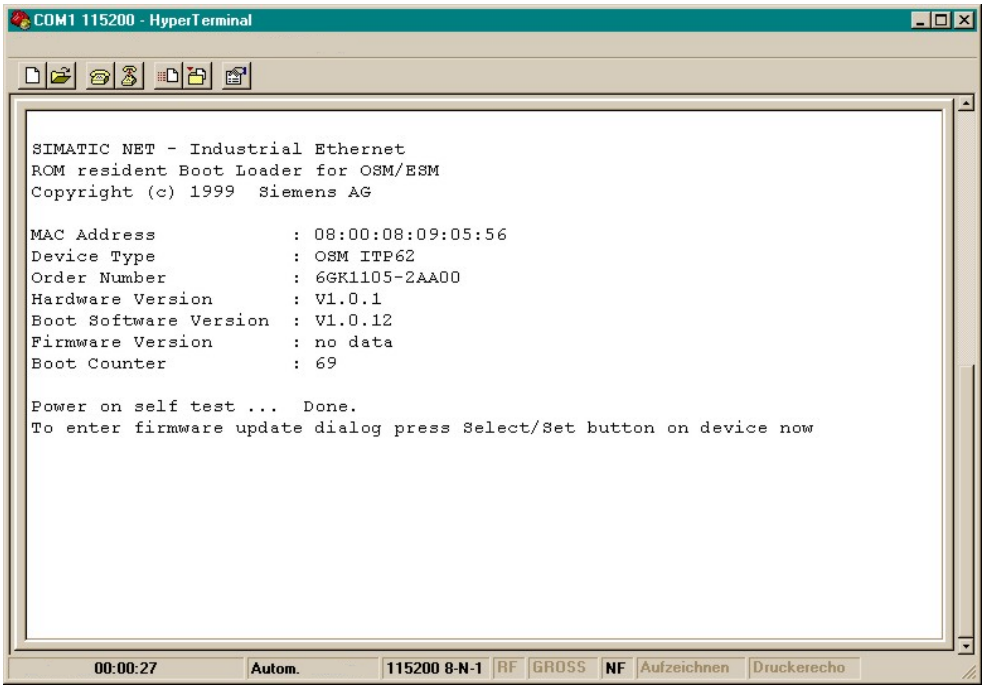


Figure 6-1

3. Press the ”Select/Set” button again briefly
4. The following prompt then appears:
   Do you really want to update your firmware? Y/N
   Confirm with Y (Yes).

The following message is then displayed in the terminal window:

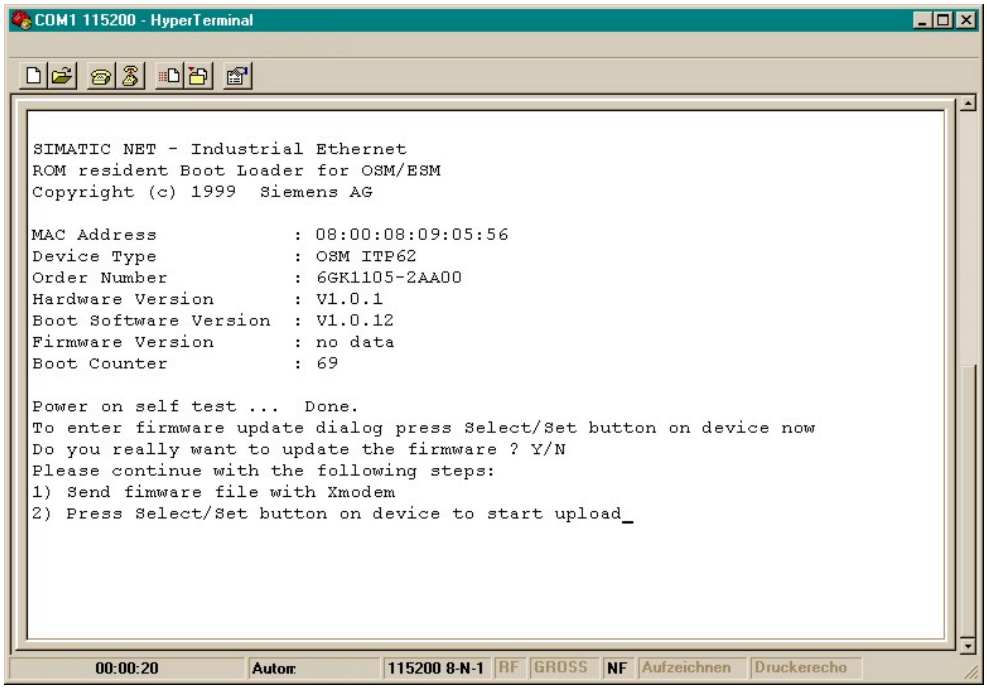


Figure 6-2

5. Now select the function Transfer > Send File function in the Hyperterminal window.
6. In the next dialog window, enter the file to be downloaded and select ”Xmodem” or “1K Xmodem” as the protocol. Start the transfer of the firmware with the ”Send” button.

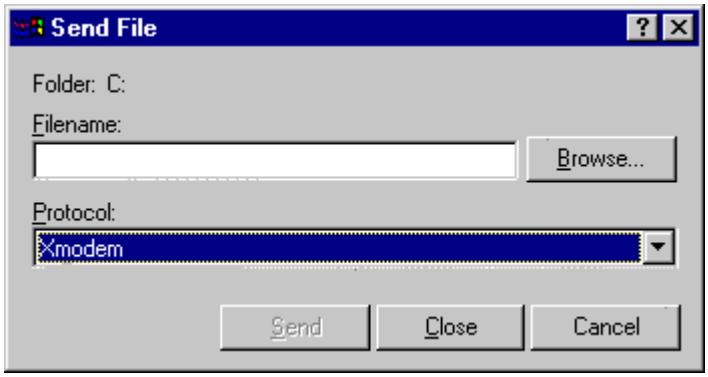


Figure 6-3

The following dialog box then appears displaying the progress of the download.

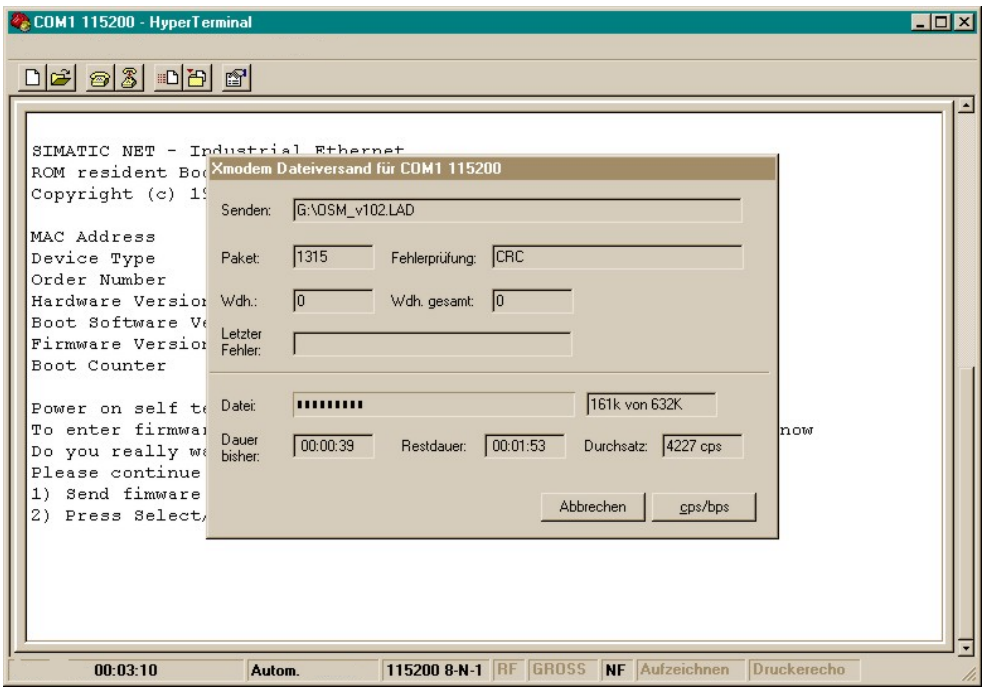


Figure 6-4

Start the download by pressing the ”Set/Select” button again.
Downloading can take up to 10 minutes. After you have downloaded the firmware successfully, the device is automatically started with the new firmware. Please note the version of the new firmware on a label on the side labeling panel of the OSM/ESM.

Note

During the download, do not interrupt the connection between the PC and OSM/ESM and do not turn off the power supply to the OSM/ESM.

If the download is interrupted by a problem on a signal line, the device will start up with the old firmware the next time it restarts. The firmware download must then be repeated.

If the firmware could not be downloaded completely to the OSM due to a power failure, the message ”Firmware in flash is faulty” appears after the device starts up. This means that the firmware must be downloaded again.

6.3 Downloading Firmware from an TFTP Server

To download firmware from a TFTP server, the server must be accessible to the OSM/ESM, see Figure 6-1.

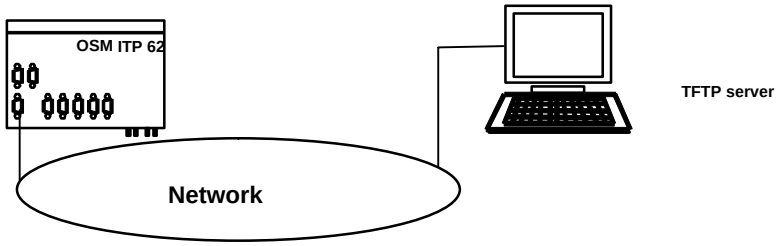


Figure 6-5 Downloading Firmware from a TFTP Server

Requirements

The following settings must also be made on the OSM/ESM, see Section 3.5 :

- The IP address, subnet mask and possibly also the gateway address must be configured on the OSM/ESM using the CLI, see Section 3.5.
- A TFTP server with an installed IETF TFTP program (RFC 1350) must exist in the network and must be accessible to the OSM/ESM. (This program is not provided by SIEMENS. It is however included with various systems and TCP/IP packages. The server can be a DOS, UNIX or Windows station.)

Note

Copy the program file to the TFTP server so that the TFTP client (OSM/ESM) has access for the download.

Downloading

Follow the steps outlined below to download the firmware:

1. Make sure that all components (OSM/ESM, TFTP server, etc.) are started up and functioning correctly.
2. Start a WBM (or CLI) session. (For more detailed information, refer to Chapter 3 or 4).
3. Make the following entries in the System menu or the in the System Save & Load window:
   - Enter the **TFTP Server IP Address** (the IP address of the TFTP server on which the new OSM/ESM firmware is located)
   - Enter the **Firmware File Name** (name and if applicable path of the file on the TFTP server containing the new OSM/ESM firmware)
   - Select the **Start Download** command.

Before the new firmware takes effect, you must restart the OSM/ESM.

Note

In the RM mode, the ring monitoring is deactivated during the TFTP download; in other words the redundancy manager cannot react to breaks in the ring during the download.

7 Notes on Troubleshooting

Table 7-1 below lists remedies if you encounter problems on the OSM/ESM.

Table 7-1 Troubleshooting

No.	Problem	Possible Cause	Remedy
1	LED **L1** and **L2** OFF	No power supply	Check the 24 V power supply.
2	LED **Fault** ON	OSM/ESM startup after turning on the power supply.	None Fault LED goes off following startup if there is no further problem.
		The fault mask does not match up with the current status of the power supplies or the port assignment.	Check the power supplies and port assignment, if necessary update the fault mask, see /1/.
		In the RM mode also:	
		Connection to a ring port interrupted.	Check the connections to the ring ports (port 3 and 4 on 4-port devices and port 7 and 8 on 8-port devices).
		Two RMs in ring simultaneously.	Turn off one RM.
		Redundant coupling, also:	
		Short-circuited or break on ITP XP standard cable 9/9.	Check the connecting cable between the standby-sync ports of the two OSMs/ESMs.
		Both OSMs/ESMs of the redundant ring coupling are set as master or both as slave.	Switch one of the devices to the master mode (Stby off), the other device to the slave mode (Stby on).
		Link down on a standby port (only when standby cable plugged in).	Check the connection to the standby ports.

Table 7-1 Troubleshooting

No.	Problem	Possible Cause	Remedy
		The firmware was not downloaded completely (power failure when saving the new firmware) or the OSM/ESM self test detected a fault.	You can recognize this state after the OSM/ESM has started up because the fault LED is lit permanently **and** the display LEDs on the front panel of the OSM/ESM do not switch over when you press the button. Download the firmware again if this problem occurred during downloading of the firmware, see Section 6 and restart the OSM/ESM. If you have not downloaded firmware, restart the OSM/ESM. If the problem persists, the OSM/ESM self test has detected a problem that it cannot eliminate. Send in the module to your SIEMENS service center for repair. Faults detected by the self test are logged if you connect a PC with the Hyperterminal program to the serial port of the OSM/ESM, see Appendix B, and run a cold restart on the OSM/ESM (power off/power on).
3	**Port Status** LED OFF, although a DTE is connected to the port.	Problem on the port, the DTE or the transmission line.	Connect the station briefly to a different OSM/ESM port and check whether the problem persists. If yes, check the transmission line to the DTE and check whether the DTE is turned on. If you are using optical cables, clean the connectors.
4	10/100 Mbps port performance low.	The partner port is not autonegotiating and is operating in the full duplex mode.	Using Web-Based Management or the CLI set the OSM/ESM port to the full duplex mode (autonegotiation disabled).
5	No connection via the serial port of the OSM/ESM to the connected PC.	Cable function, incorrectly set Hyperterminal program on the PC, incompatible transmission rate.	Check the cable. Check the settings in the Hyperterminal program. Check the transmission rate (default 115 Kbauds).
6	No access to CLI commands.	Access only with administrator password.	Enter **admin** as the login and then enter the administrator password (the default is **admin**).
7	No IP connections.	The IP address was not assigned.	Set the IP address and subnet mask using the CLI.

Table 7-1 Troubleshooting

No.	Problem	Possible Cause	Remedy
8	Fault Status signals “non recoverable ring error”	The RM is receiving test frames on the OSM ring from only one direction. This is caused by defective devices or cables in the OSM ring.	Check whether cable and devices function correctly. Problem indicators are the traffic LEDs and the statistics counters of the ring ports.
9	No E-mail, BOOTP/DHCP, RMON, or TELNET connection.		Check/activate E-Mail, BOOTP/DHCP, RMON or TELNET. RMON is not available on the OSM TP22 and ESM TP40.
10	No reaction from Web-Based Management.	No IP connection	Check the IP connection with the **Ping** command. (Entry in MS-DOS as ping <IP address>, for example ping 142.11.7.8). The ping check whether the OSM/ESM is accessible from the PC.
		Incorrect browser connection	See Appendix A
		SNMP disabled	Run the **snmp E** command via the CLI.
11	Power supply failure	Bad network configuration	Make sure that there are no loops within the network.
12	Password error	Incorrect password.	If you forget the password, you can activate the default passwords again by pressing the button on the front panel of the OSM/ESM to start a reset.
13	TFTP process abort.	The TFTP server terminates the process due to a timeout.	Increase the timeout time for the TFTP server.

Internet Browser Settings

A

To use Web-Based Management with the OSM/ESM, you must make the correct settings in the Internet browser. This appendix contains instructions for making the settings for the Internet browsers shown in Table A-1 below. You can use this procedure as the basis for setting other Internet browser versions. Web-Based Management of the OSM/ESM was tested with these Internet browsers.

Table A-1 Internet Browser

Browser	
Microsoft Internet Explorer	Netscape Communication Navigator
5.0, 5.5 and 6.0	4.7, 6.1 and 6.2

Note

The Web Based Management of the OSM/ESM has been tested with certain combinations of browsers and Java Virtual Machines (JVM). Only the JVM supplied and installed with the product was tested with Netscape and only the JVM for Microsoft was tested with the Internet Explorer. We recommend that you only use one of these combinations. The JVM from Microsoft must be installed separately according to the Version of Internet Explorer (download from Microsoft Web pages).

A.1 Microsoft Internet Explorer 6.0

You can check whether or not you have the Internet Explorer 6.0 as follows:

1. Select Help (?) ->about Internet Explorer to open the window shown in Figure A-1.

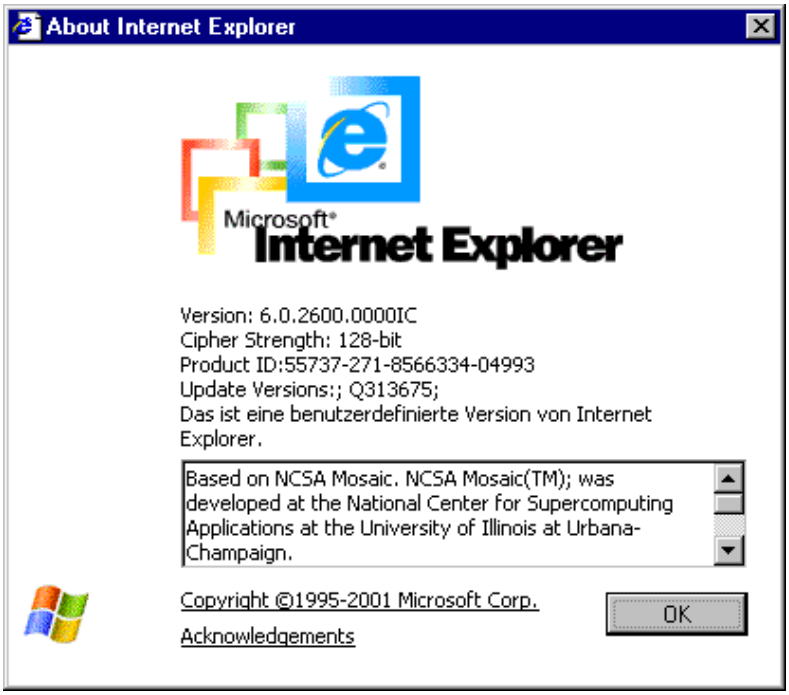


Figure A-1 Microsoft Internet Explorer 6.0 - about Internet Explorer Window

2. Select *Tools -> Internet Options -> Security* to open the window in Figure A-2.
3. Select “Trusted Sites” in the zones box and click the “Sites...” button.

4. Add the IP address of the OSM/ESM to the zone of trusted sites after clicking the Sites button to open the window shown in Figure A-2.

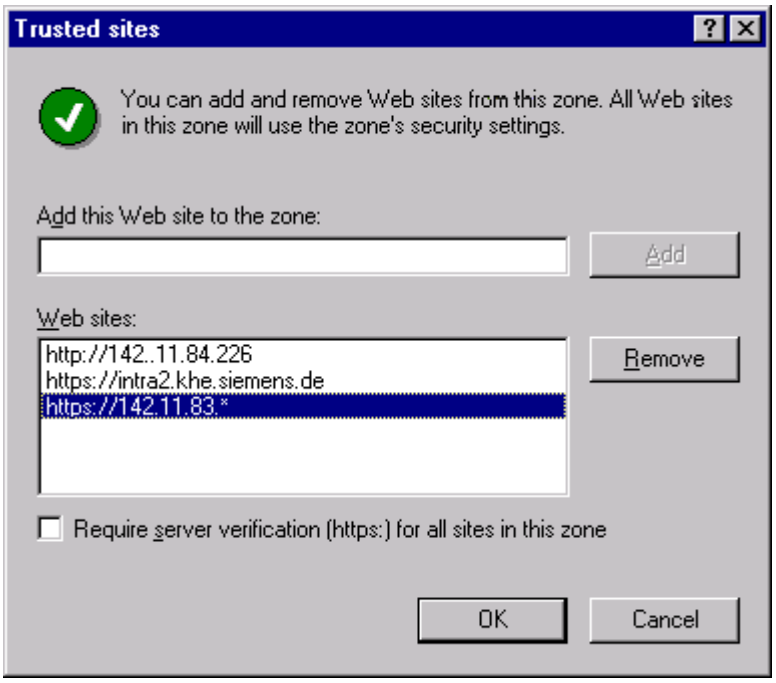


Figure A-2 Trusted Sites

Note

Please note that for the adress input for OSM/ESM in “trusted sites” the adress does not beginn with https:// but with http://.

5. Enter the IP address of the OSM/ESM as shown in Figure A-3. You can use wildcards (*) to enter entire address ranges for several OSMs/ESMs. If you enter, for example, 142.11.83.*, the addresses 142.11.83.0 to 142.11.83.255 are added to the trusted sites.

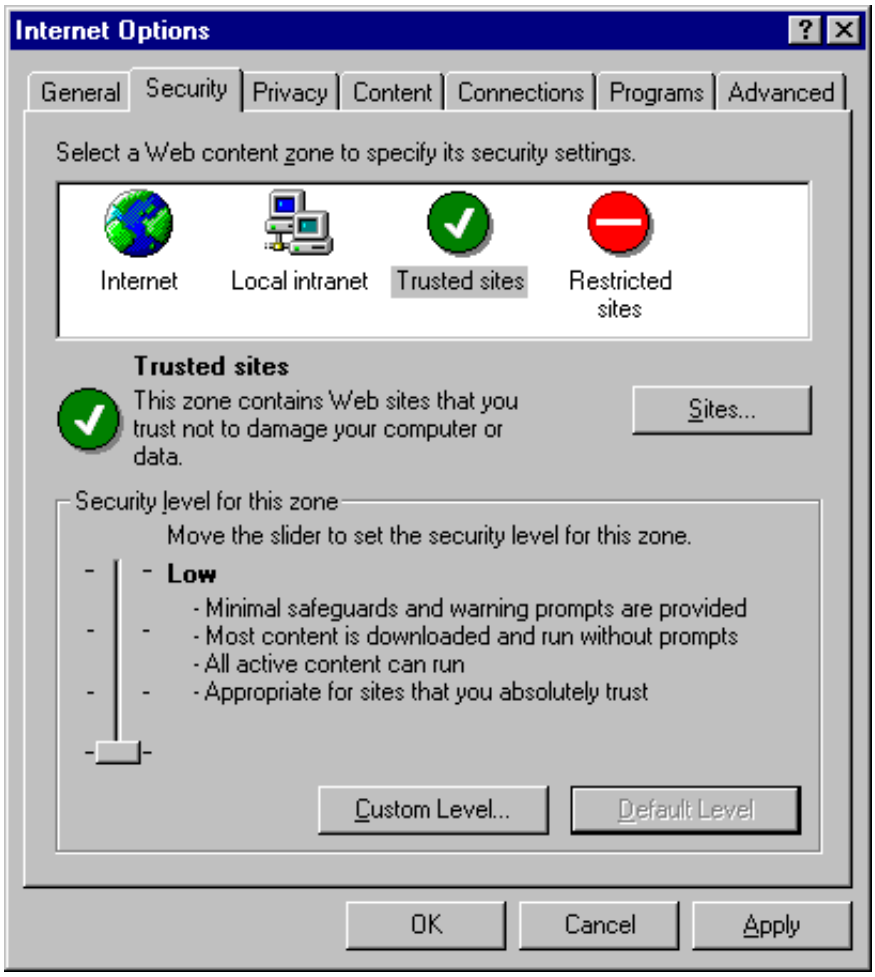


Figure A-3 Microsoft Internet Explorer 6.0 - Internet Options Window

6. Click the *Custom Level* button to open the window shown in Figure A-3.
7. Set the *Java permissions* to *Custom* as shown in Figure A-4.

8. Activate *Active Scripting*, see Figure A-4.

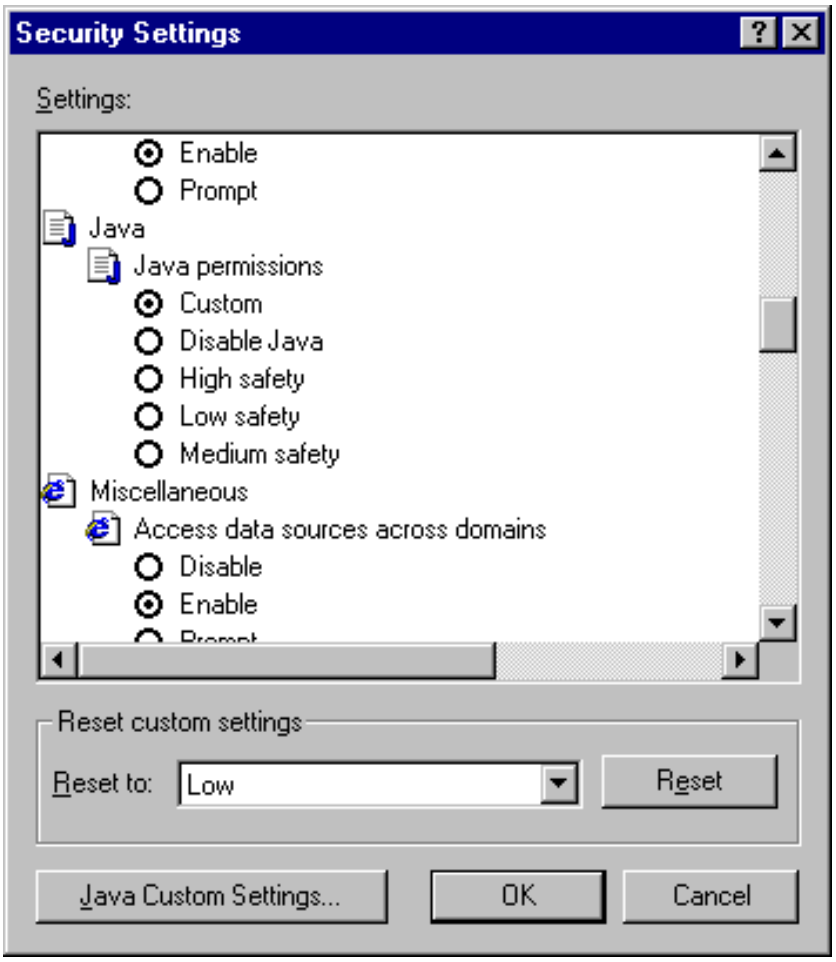


Figure A-4 Microsoft Internet Explorer 6.0 - Security Settings Window

9. Click the *Java Custom Settings* button as shown in Figure A-4 to open the window shown in Figure A-5.
   (If this button is not displayed, you have not selected the custom Java permissions as shown above.)

10. Open the *Edit Permissions* window, see Figure A-5. If you cannot make any modifications in this window, contact your network administrator. (It is possible that you do not have the required permissions or that your browser must be updated.)
11. Make sure that *Run Unsigned Content* is activated (or at least *Run in sandbox* , *Access to all Network Addresses* and *Dialogs* are activated).

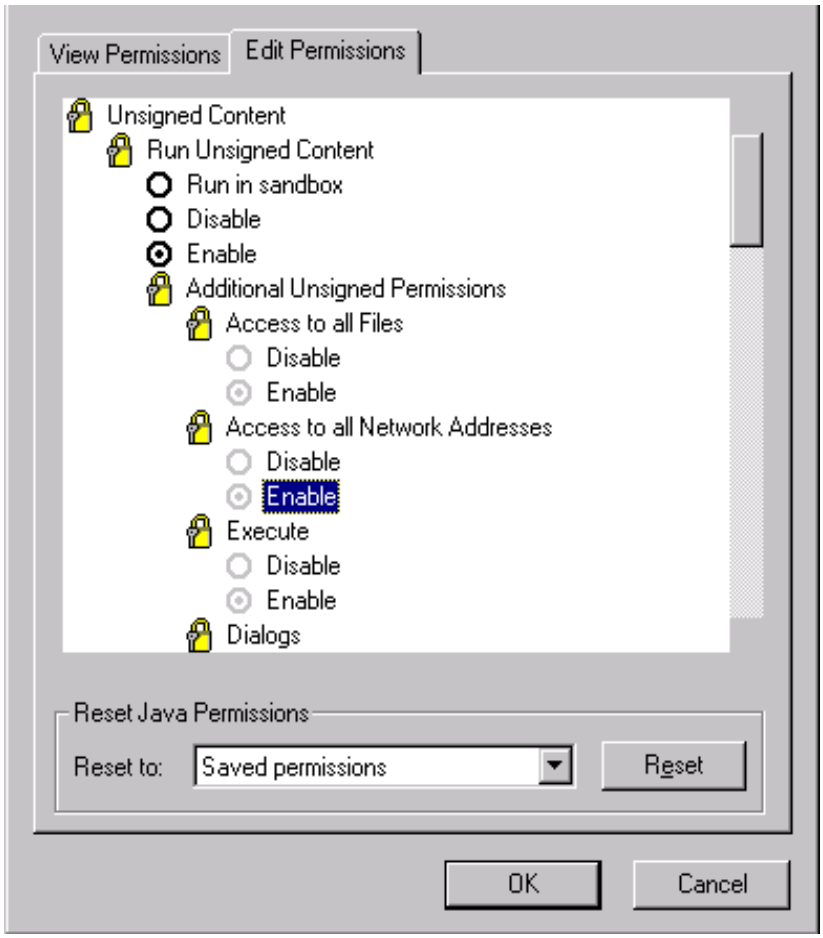


Figure A-5 Microsoft Internet Explorer 6.0 - Edit Permissions Window

12. Select *Tools -> Internet Options -> Advanced* to open the window shown in Figure A-6. Make sure that *Java logging* and *Java JIT compiler* are activated. (*Java console* can also be enabled.)

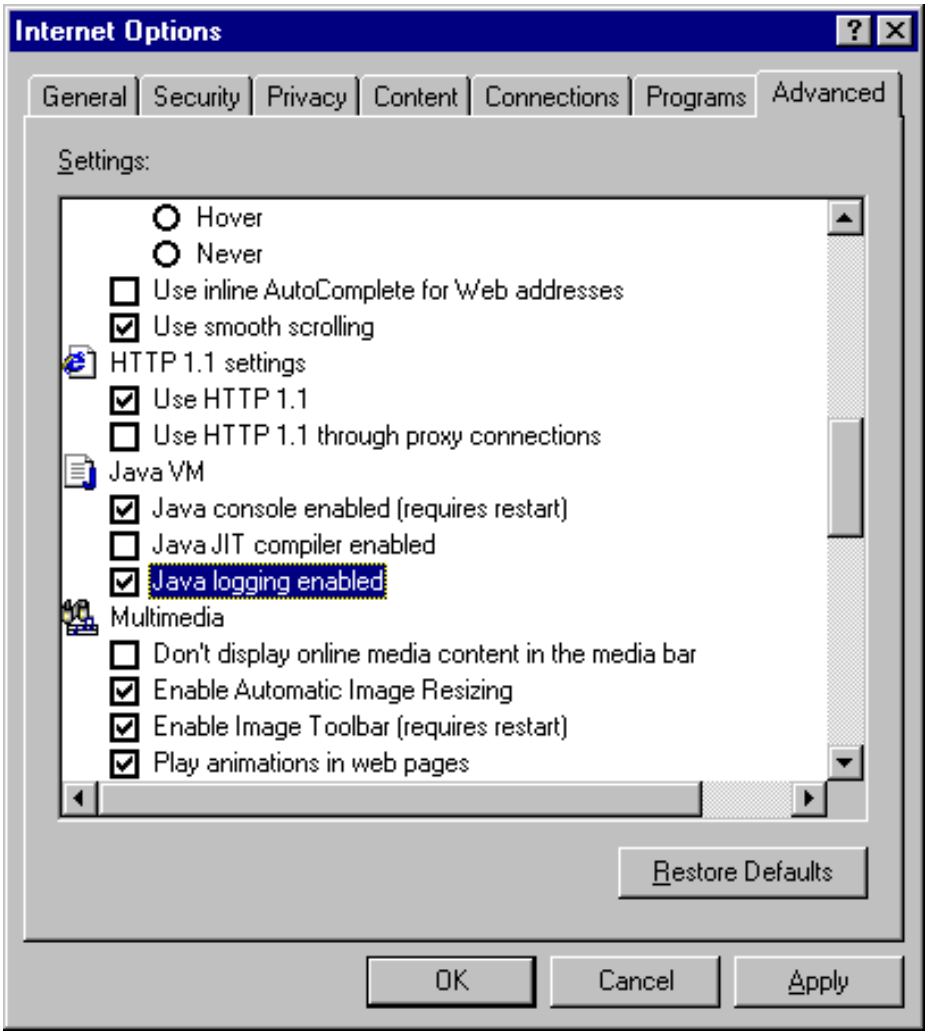


Figure A-6 Microsoft Internet Explorer 6.0 - Advanced Internet Options Window

13. If you use a proxy server that only accepts DNS registered IP addresses and your OSM/ESM is not DNS registered, you may need to connect directly to the OSM/ESM.
    You do this by selecting *Options ->Internet Options->Connections,* to open the window shown in A-7. Click the *LAN Settings* button in this window to open the window shown in Figure A-8.

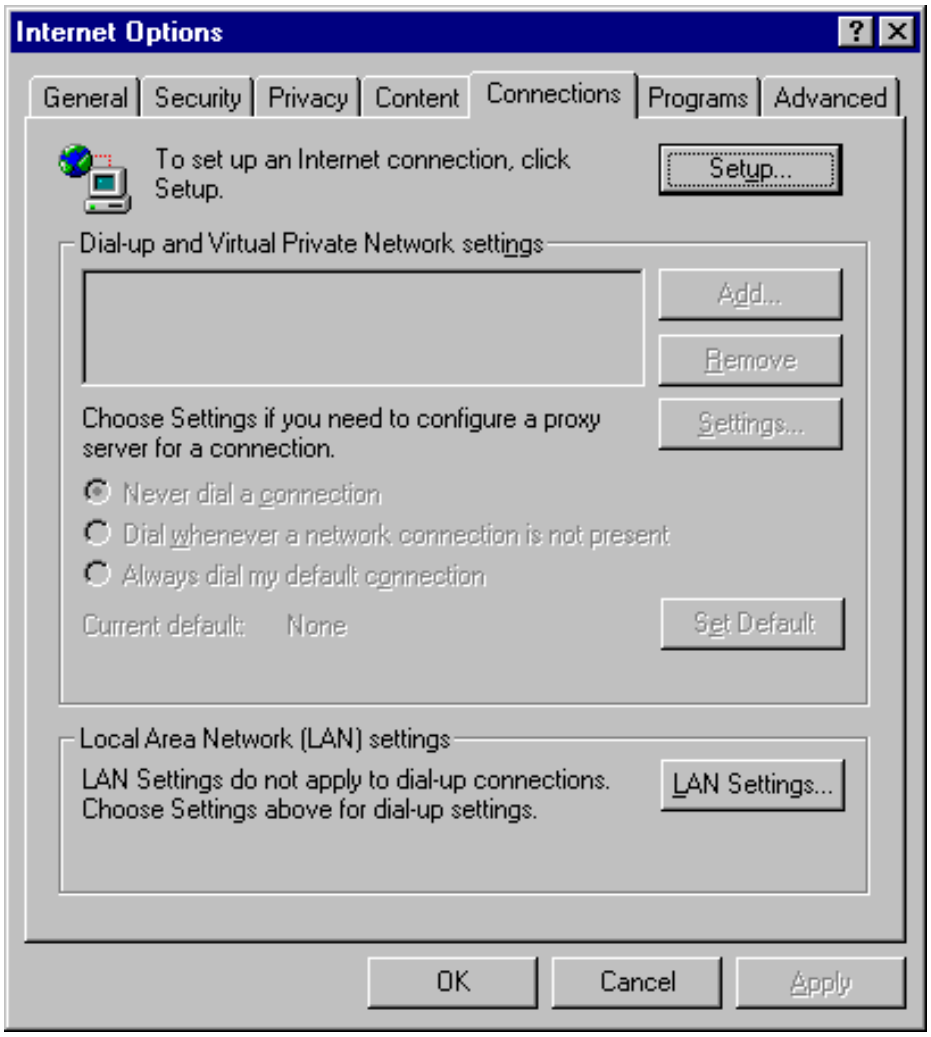


Figure A-7 Microsoft Internet Explorer 6.0 - Connections Window

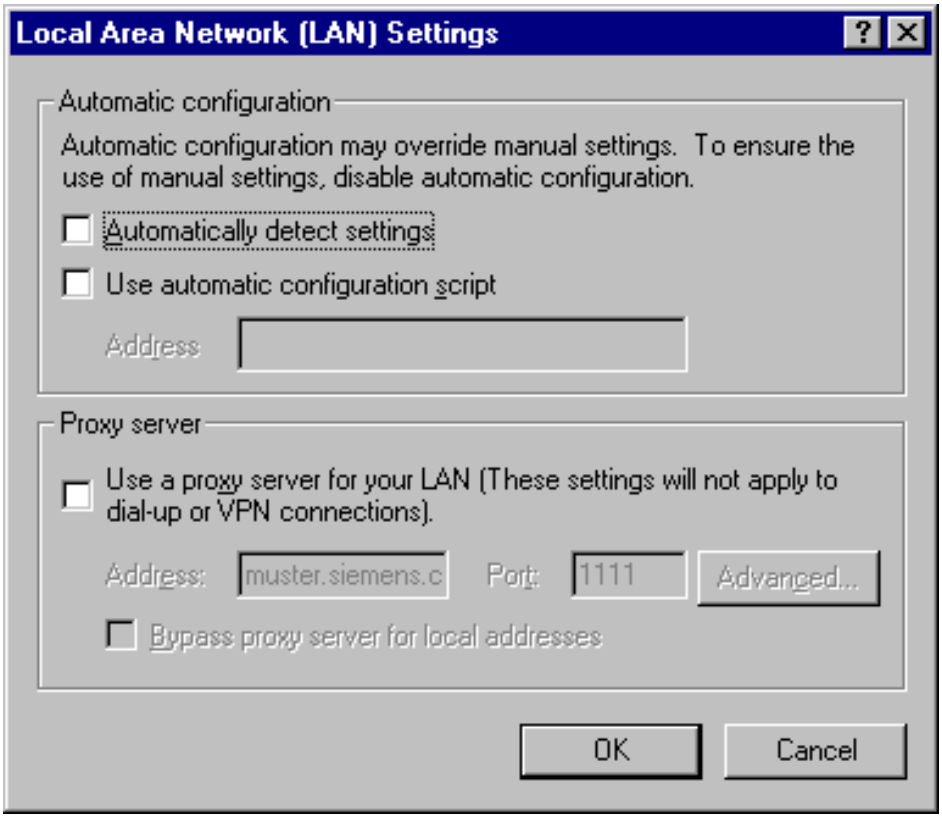


Figure A-8 Microsoft Internet Explorer 6.0 - LAN Settings

14. In this window, deactivate the proxy server by clicking the *Use Proxy Server* check box or click the ”Advanced” button to open the window shown in Figure A-9 in which you can enter the addresses for which the proxy server will not be used.

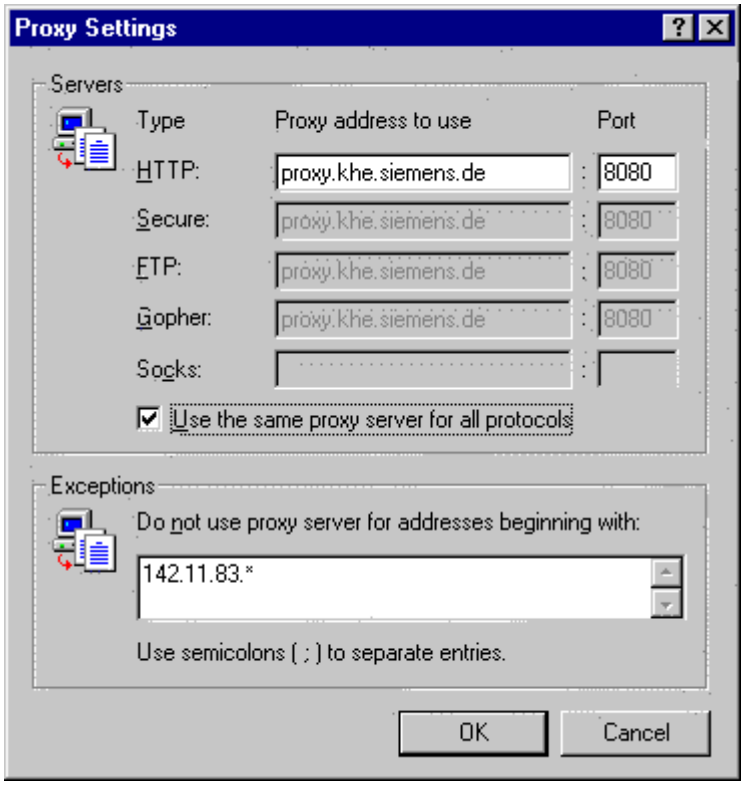


Figure A-9 Proxy Settings

15. In this window, enter the address of the OSM/ESM; you can also enter address ranges using wildcards. If you enter 142.11.83.*, for example, no proxy server is used for addresses 142.11.83.0 to 142.11.83.255.

A.2 Netscape Communicator 6.2

1. Select Edit -> Settings -> Advanced to open the window shown in Figure A-10.
2. Select *Activate Java* and *Activate JavaScript for Navigator*.

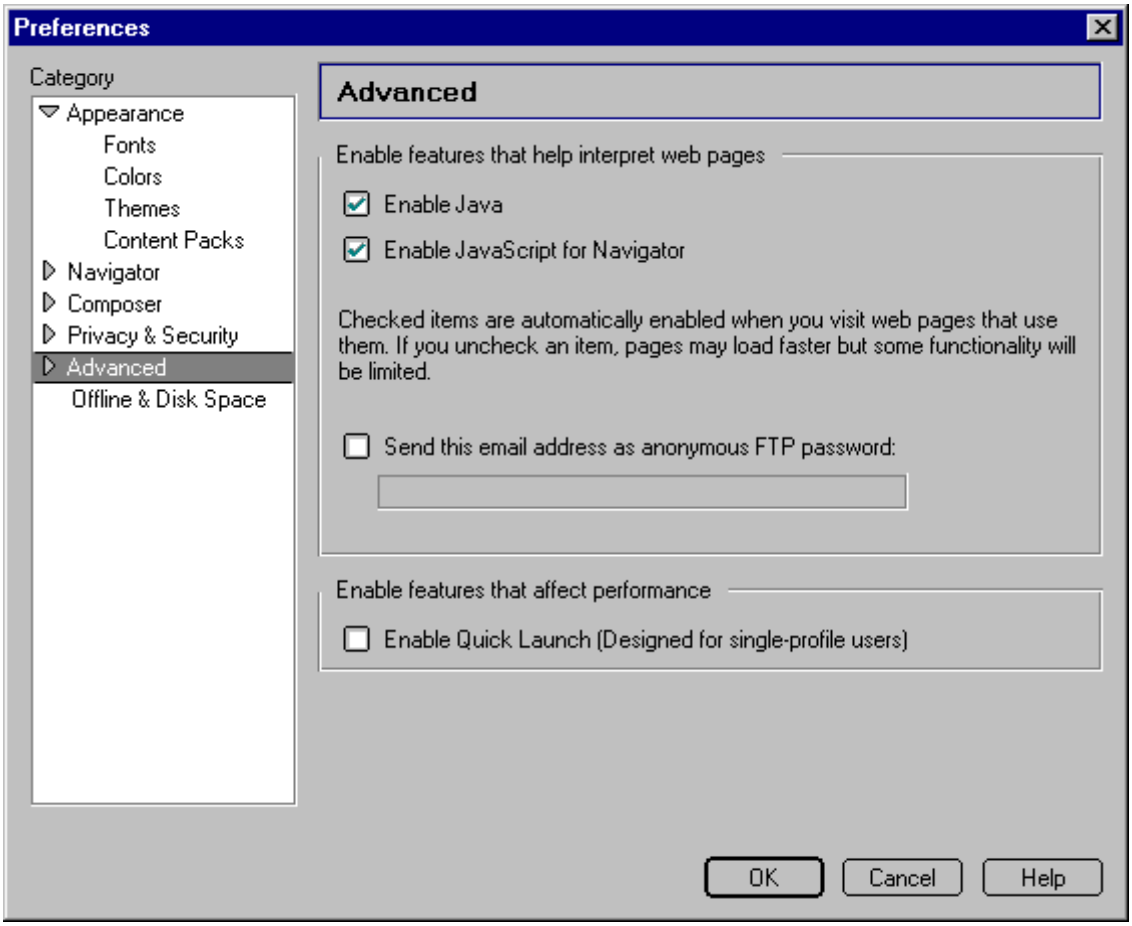


Figure A-10 Netscape Communicator/Navigator 6.2 - Advanced Settings Window

If you use a proxy server that only accepts DNS registered IP addresses and your OSM/ESM is not DNS registered, you may need to connect directly to the OSM/ESM.

To do this, select *Edit -> Settings -> Advanced -> Proxies* to open the window shown in Figure A-11 and set *Direct connection to Internet*.

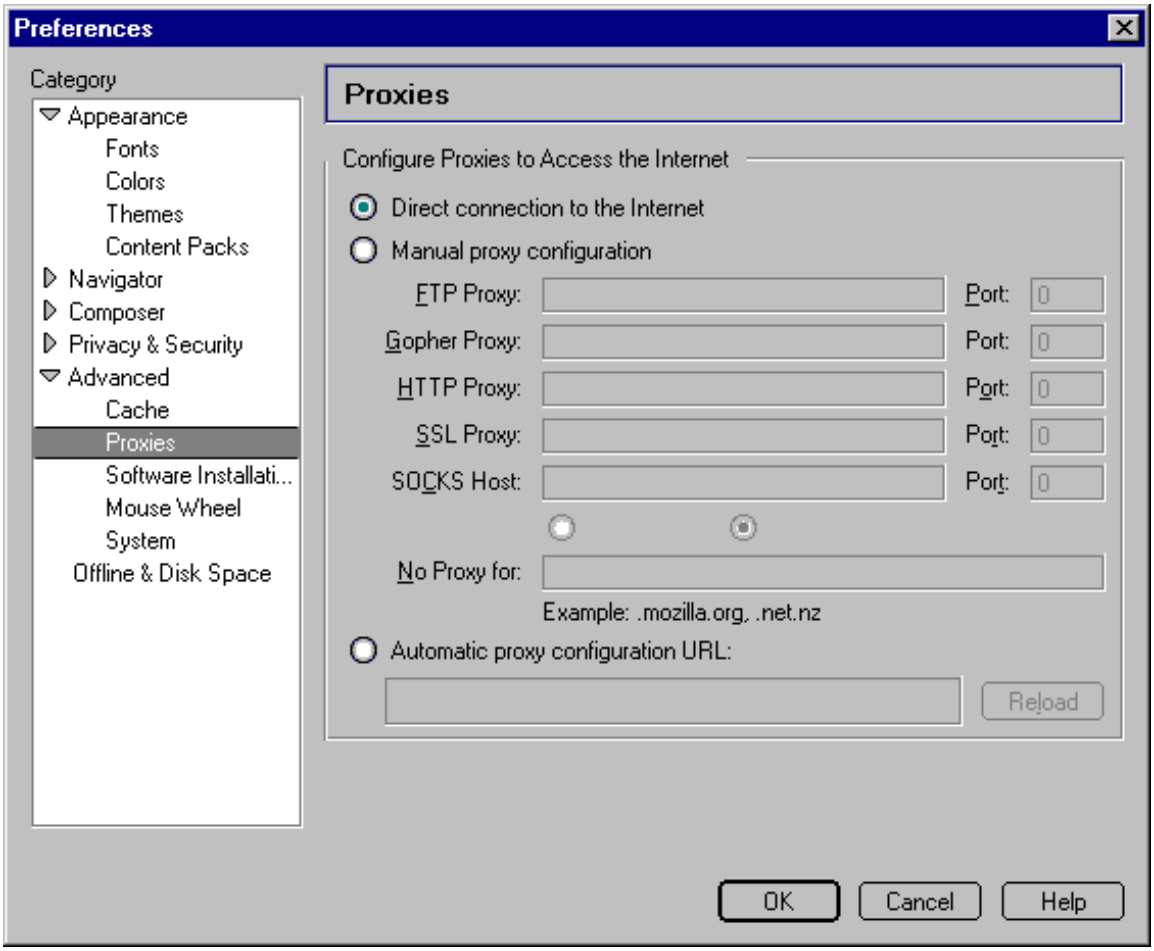


Figure A-11 Netscape Communicator/Navigator 6.2 - Proxy Settings Window

Connecting a PC with Hyperterminal to the Serial Port of the OSM/ESM

B

You require a PC with the Hyperterminal program (available with Windows 95/98 NT/2000 in Programs -> Accessories) if you want to download the OSM/ESM firmware via the serial port or want to use the command line interface (CLI). Follow the steps outlined below to connect a PC with the Hyperterminal program to the OSM/ESM:

Connect the serial interface of your PC and the OSM/ESM with a normal null modem.

Depending on the port of the PC that you are using, you require a cable with a 9-pin or 25-pin sub-D female connector for the PC end, and a 9-pin female connector for the OSM/ESM end.

Table B-1 below shows the pinning and connection of the two cable variants.

Table B-1 Pinning and Connections

PC port	**25-pin female**	**9-pin female**	**Connected to**	**OSM connector 9-pin female**	
Signal name	Pin	Pin		Pin	Signal name
TD (Transmit Data)	2	3	_____	2	RD
RD (Receive Data)	3	2	_____	3	TD
RTS (Request To Send)	4	7	_____	8	CTS
CTS (Clear to send)	5	8	_____	7	RTS
SG (Signal Ground)	7	5	_____	5	SG
DSR (Data Set Ready)	6	6	_____	4	DTR
DTR (Data Terminal Ready)	20	4	_____	6	DSR

Note

Please note that the serial port on some SIMATIC programming devices is a 25-pin female connector. If this is the case, use a gender changer (25-pin male to 25-pin male) available from PC dealers.

Follow the steps outlined below in Hyperterminal:

1. Create a new connection (for example with File -> New Connection).
2. Make the settings in the Properties dialog as shown below.

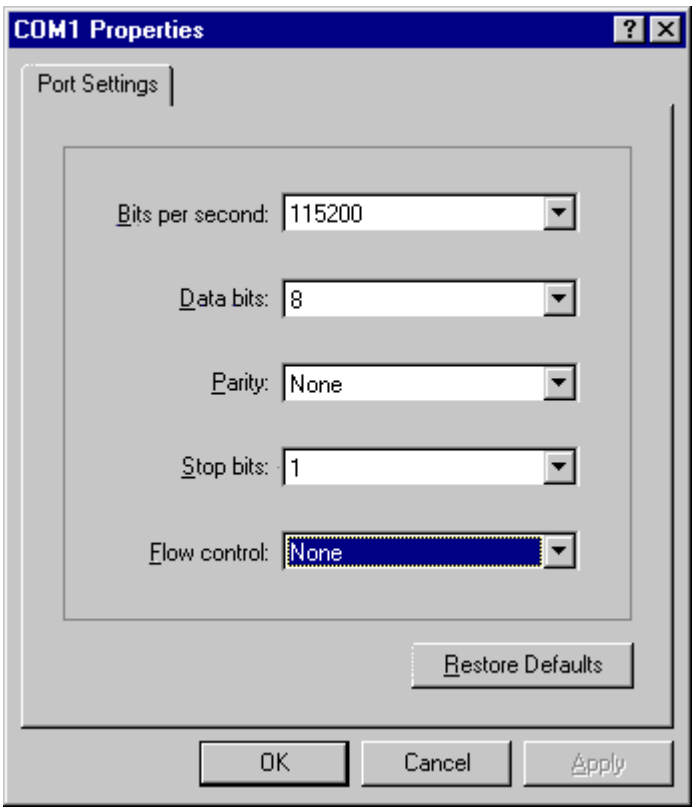


Figure B-1 Properties Tab

References

C

/1/ SIMATIC NET Industrial Ethernet OSM/ESM Operating Instructions, supplied with every device on CD and available at
http://www4.ad.siemens.de/view/cs/en/8676999
on the Web.

/2/ SIMATIC NET Industrial Twisted Pair and Fiber-Optic Networks, Release 05/2001.

Order numbers:

6GK1970-1BA10-0AA0 German
6GK1970-1BA10-0AA1 English
6GK1970-1BA10-0AA2 French
6GK1970-1BA10-0AA4 Italian

Abbreviations/Acronyms

D

Abbreviation/ Acronym	Definition
ASCII	American Standard Code for Information Interchange
BOOTP	Bootstrap Protocol
CLI	Command Line Interpreter
CRC	Cyclic Redundancy Check
CSA	Canadian Standards Association
CSMA/CD	Carrier-Sense Multiple Access with Collision Detection
DHCP	Dynamic Host Configuration Protocol
DNS	Dynamic Name System
ESM	Electrical Switch Module
FDB	Filtering Data Base
GUI	Graphical User Interface
HTML	HyperText Markup Language
HTTP	HyperText Transfer Protocol
ID	IDentity
IEEE	Institute of Electrical and Electronics Engineers
ITP	Industrial Twisted Pair
IP	Internet Protocol
LAN	Local Area Network
MAC	Media Access Control
MAU	Medium Attachment Unit
MDI	Medium Dependent Interface (*Pinning:* 1→RX+, 2→RX-, 3→TX+, 6→TX-)
MDIX	Medium Dependent Interface with cross-wiring (*Pinning:* 1→TX+, 2→TX-, 3→RX+, 6→RX-)
MIB	Management Information Base
NIC	Network Interface Card
NMS	Network Management Station
OS	Operating System
OSM	Optical Switch Module
POST	Power-On SelfTest
RFC	Request For Comment
RM	Redundancy Manager
RMON	Remote MONitoring

Abbreviation/ Acronym	Definition
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
TCP/IP	Transmission Control Protocol over IP
TELNET	(dial-up) TELephone NETwork (connection protocol)
TFTP	Trivial File Transfer Protocol
TP	Twisted Pair
UDP	User Datagram Protocol
URL	Universal Resource Locator
UTP	Unshielded Twisted Pair
WBM	Web Based Management

Glossary

Autocrossover

Capability of automatically crossing over the send and receive signals at twisted-pair ports (automatic switchover between MDI and MDI-X pinning at a port). When, for example, connecting network components, you no longer need crossover cables.
The autocrossover function is available only when autonegotiation is activated.

Autonegotiation

In the autonegotiation mode, an electrical OSM/ESM port sets itself automatically to the transmission rate (10/100 Mbps) of the connected partner device. If the partner device also supports autonegotiation, the devices further negotiate whether they will exchange data in the half-duplex or full-duplex mode and full-duplex flow control see Section 2.12.

FDB table

The FDB table contains node addresses (MAC addresses) and the port of the OSM/ESM over which the node address is obtainable.

Aging

Aging means that a learned entry in the FBD table is cleared when no packet with a source address corresponding to the entry is received within the aging time. The OSM/ESM assumes that this node no longer exists.

Back pressure

Flow control for ports operating in the half duplex mode. With this type of flow control, the OSM/ESM reduces the packet rate received at a port if there is overload in the network by generating additional collisions.

BOOTP

The Bootstrap protocol is used by the OSM/ESM to download the IP address, subnet mask and address of the default gateway automatically from a BOOTP server. It is also possible to send the name of a file containing the firmware on the TFTP server.

Boot software

The boot software is software integrated on the OSM/ESM that is required to download the OSM/ESM firmware. The boot software cannot be reloaded.

Boot version

Version of the boot software.

Broadcast address

Packets with a broadcast address can be read by all nodes in the LAN (destination address FF:FF:FF:FF:FF:FF).

CLI

Command line interface (see Command interpreter).

Collision

A collision occurs when two DTEs attempt to send at the same time. The collision is handled according to the procedures defined in IEEE 802.3.

Command interpreter

The command interpreter (CLI) of the OSM/ESM interprets the terminal entries and executes the corresponding commands.

CRC

Cyclic **R**edundancy **C**heck - This is used in data transfer protocols to be able to detect transmission errors (CRC errors) in received packets.

Default

Factory default settings on the OSM/ESM.

Default gateway

The default gateway passes on all packets that are not addressed to stations in the same LAN (subnet).

DNS server

Every computer attached to the Internet has its own unique IP address. So that LAN/Internet users do not need to learn the numbers to be able to access a particular computer in the network, many IP addresses are assigned alphanumeric names that are managed by DNS servers.

ESM

SIMATIC NET Industrial Ethernet Electrical Switch Module (has only electrical ports).

Event log table

A table in which certain events detected by the OSM/ESM are stored in non-volatile memory for diagnostic purposes. The log table of the RMON MIB is stored under events and is therefore a dynamic part of the MIB.

Fault mask

The fault mask is used with the OSM/ESM to mask out certain fault events. Events that are not masked cause the signaling contact to respond and are displayed by the fault LED.

Filtering database (FDB)

See FDB table

Firmware

Module software, in this case software running on the OSM/ESM.

Firmware version

Version of the OSM/ESM firmware

Flow control

A function on the OSM/ESM with which the number of packets received at the OSM/ESM can be reduced in case of overload to reduce the risk of packet loss.

Full duplex mode

An OSM/ESM port operating in the full duplex mode can receive and send data at the same time.

Full duplex flow control

The full duplex flow control of the OSM/ESM operates in compliance with the IEEE 802.3x standard. If there is overload, the OSM/ESM generates pause packets that stop or re-enable the sending of new packets by the connected partner device. The partner device must support full duplex flow control.

Half duplex

An OSM/ESM port operating in the half duplex mode cannot receive and send data at the same time. Data can only be received and sent alternately.

Half duplex flow control
see Back pressure

HTML
HTML is the abbreviation for Hypertext Markup Language. Using this language it is possible to publish documents in a uniform language on the Web. The main feature of this language is the ability to specify connections to other HTML documents known as URLs.

IP address
An IP address consists of a numeric code made up of four numbers from 0 to 255 (for example 192.168.0.55). This is the numeric address of a specific computer in the network/Internet.

Jabbers
Packets with an invalid CRC and a length greater than 1536 bytes.

Java
Programming language developed by Sun.

Java applet
The name for a Java subroutine. On the OSM/ESM, there is a Java applet in the Web site of the OSM/ESM that updates the device status shown on the Web site after startup.

Learning
The OSM/ESM automatically learns the MAC addresses and port numbers of the nodes connected to it and stores the information in the FDB table.

Link status
The valid link from an OSM/ESM port to the port of a partner device is monitored by link test pulses. A valid link is indicated on the OSM/ESM, for example by the port status LED being lit (permanent green light).

MAC address
6-byte node address of an Ethernet node.

MIB
Management Information Base. In network management, the database (tree structure) in which all objects and variables that can be managed are entered.

Mirroring

Mirroring allows you to mirror (copy) the bi-directional data traffic to an OSM/ESM port (mirrored port) to another OSM/ESM port (monitor port) and to record it with a commercially available protocol analyzer for diagnostic purposes.

Multicast address

A packet with a Multicast address can be received by several nodes prepared to accept this address.

Operative software

see firmware

OSM

SIMATIC NET Industrial Ethernet Optical Switch Module (includes optical and electrical ports).

Oversize packets

Packets with a valid CRC and a length (packet size, see below) greater than 1536 bytes.

Packet size

Length of a packet from the destination address to the CRC field inclusive.

Partition mode

If more than 60 collisions occur during transmission, the OSM/ESM changes to the Partition mode. It waits for the first valid package before it returns to the normal transmission mode. In the Partition mode, it continues to send but no longer receives (partitioned).

Port

(Ethernet) interface of the OSM/ESM

Port locking

Locking is used to ensure that only packets from authorized stations are passed on via the OSM/ESM, see Section 2.6.

Port name

A name that can be assigned to every port of an OSM/ESM in the network management system.

Power line 1/2

Power supply line 1/2 of the OSM/ESM.

Redundancy manager (RM)

The OSM/ESM operating as the redundancy manager monitors the line of OSMs/ESMs attached to it. If there is a break on the line, it switches through and therefore recreates a functioning bus configuration.

Restart

The OSM/ESM can be restarted by the management system (Web Based, CLI, SNMP).

RM mode

This indicates whether or not an OSM/ESM is operating in the redundancy manager mode (RM on).

RM status

Indicates whether an OSM/ESM operating as the redundancy manager has switched the bus connection through (RM active) or not (RM passive).

Remote MONitoring (RMON)

The RMON agent of the OSM/ESM collects data, for example, on network load that can be queried by a network management station. The OSM/ESM supports the RMON groups: Statistics, History, Alarm, Event.

RFC

Request for Comment - Standardization document of the Research and Development group of the Internet, for example for defining protocols, procedures and services.

RFC 1213

Specifies the MIB II that must be supported by all devices that can be managed using SNMP. RFC 1213 can be downloaded from the Internet.
http://www.faqs.org/rfcs/rfc1213.html

Serial baud rate

Baud rate of the serial port of the OSM/ESM. The default is 115 Kbauds. The baud rate can be changed by SNMP or Web-Based Management.

Signaling contact

Binary contact used with SIMATIC NET network components to signal fault events.

SMTP server

(Simple Mail Transfer Protocol Server) computer that receives sent mails and passes them on to the recipient.

SNMP

Simple Network Management Protocol, nonproprietary LAN management standard.

Standby cable

Connecting cable (ITP XP standard cable 9/9) for linking the standby master and standby slave in a redundant coupling.

Standby configuration error

Error in the configuration of the redundant coupling, see /1/, for example faulty or undetected standby connecting cable.

Standby master

An OSM/ESM in the redundant coupling that handles the coupling of the connected networks in normal operation.

Standby mode

This is activated by a DIP switch on the OSM/ESM and indicates whether or not an OSM/ESM is operating as the standby slave (Stby on).

Standby slave

An OSM/ESM in the redundant coupling that takes over the coupling of the attached networks if an error occurs.

Standby status

This indicates whether or not the standby master or the standby slave has taken over the coupling of the connected networks in the redundant coupling. Standby active: The device has taken over the coupling. Standby passive: The device has not taken over the coupling.

Static address

Static address stored in the OSM/ESM FDB table (non-volatile). Such addresses can be configured by the user with Web management or using SNMP.

Subnet mask

The subnet mask decides which part of the IP address is used as the subnet address. In a Class B network (subnet mask 255.255.0.0), the first two fields of an IP address (for example 150.215 of the IP address 150.215.017.009) represent the subnet.

System contact

An SNMP MIB object. Includes contact person/address (for example the maintenance technician responsible) for a device (maximum of 64 characters). This can, for example, be written using Web-Based Management.

System location

An SNMP MIB object containing information about the location of a device (maximum 64 characters). This can, for example, be written using Web-Based Management.

System name

An SNMP MIB object. The domain name of the OSM/ESM can be entered in this field (maximum 64 characters). This can, for example, be written using Web-Based Management.

Sys Up time

This is the time since the OSM/ESM was turned on.

TELNET

Standard protocol for remote login. Allows an interactive connection to be established to another device via a LAN or the Internet as if directly connected to the device via a terminal.

TFTP server

In conjunction with this server, the OSM/ESM can provide the following functions over TFTP (Trivial File Transfer Protocol):

- Download new firmware from the server to the OSM/ESM
- Save the OSM/ESM configuration on the server
- Load the OSM/ESM configuration from the server
- Save the OSM/ESM log table file on the server

Trap

If certain events occur, the OSM/ESM can generate (SNMP) trap messages and send them to different nodes, for example management stations. These traps contain error messages in plain language that can be displayed by a management station.

Unicast address

A packet with a Unicast (destination) address is intended for only one node with the corresponding MAC address.

Undersize packets

Packets with a length of less than 64 bytes.

WAN

Wide Area Network

WBM

Web-Based Management - Diagnostics and configuration using a Web browser.

A

Address type, 4-40
Administrator, 3-2
Agent , 1-2
Aging, 2-6, 4-37
Aging time, 2-6, 4-37
Alarm, 5-3
Autocrossover, 2-3
Autonegotiation, 2-2

B

BOOTP, 2-14, 4-28

C

CLI commands, 3-5
Command interpreter, 1-8, 3-2, 3-3
Current FDB table, 4-38

D

Data window, 4-8
Default gateway, 4-28
Device status field, 4-8
DHCP, 1-8, 2-14, 2-22, 3-12, 4-3, 4-28, 7-4
Duplicity, 2-3

E

E-mail, 2-10, 4-27, 4-31
Event, 5-3
Extended redundant ring configuration, 2-18

F

Factory Defaults, 2-4
Factory defaults, 2-4
Fault mask, 4-21
Fault mask , 4-21
Fault status, 4-20
FDB, 2-5
FDB table, 2-5
Firmware download, 6-3, 6-6
Flow control, 2-13, 4-37

G

Group members , 4-44

H

History, 5-3

I

Internet browser, 4-2
IP address, 4-28

L

Learned, 4-39
Learned addresses, 2-5
Lock disabled, 2-7
Lock enabled, 2-7
Locking, 2-7

M

MAC address, 4-40
MAC address , 4-38
Management system, 1-2
Memory defaults, 2-4
Menu tree, 4-8
MIB, 1-4, 5-2
Microsoft Internet Explorer, 4-3
Mirrored port , 4-36
Mirroring, 2-8, 4-36
Monitor port, 4-36
Multicast, 4-40

N

Netscape Communicator, 4-3
Network management protocol, 1-2

P

Password, 4-5
Password protection, 3-2
Port list, 4-40

Port pool, 4-44
Power line 1 , 4-19
Power line 2, 4-19
Power monitoring, 4-21
Protected settings, 2-4

R

Redundant ring configuration, 2-17
RM active state, 4-25
RM mode, 4-19
RM status, 4-19
RMON, 4-27
RMON groups, 5-3

S

Serial port baud rate, 4-11
Set new values, 4-11
Signaled faults, 4-25
SMTP, 4-31
SMTP server, 4-31
SNMP, 1-2, 1-3, 5-2
Standby active state, 4-26
Standby cable, 4-18
Standby mask, 4-23
Standby master, 2-17, 4-23
Standby mode, 4-18
Standby ports, 4-23
Standby slave, 2-17, 4-23
Standby status, 4-19
Standby sync ports, 2-17
Static, 4-39
Static addresses, 2-5
Static FDB table , 4-40
Statistics, 5-3
Statistics counters, 4-49
Subnet mask, 4-28
System contact, 4-10
System description, 4-10
System location, 4-10
System name, 4-11
System restart, 4-13
System up time, 4-10

T

TELNET, 3-3, 4-27
Test packets, 4-26
TFTP server, 6-6
Transmission rate, 2-3
Traps, 2-9, 4-28, 4-33

U

UDP, 1-3
Unicast, 4-40
User, 3-2

V

Version numbers , 4-11

W

Web-Based Management, 4-2